NBG334W

Интернет-центр для подключения по выделенной линии Ethernet с точкой доступа Wi-Fi 802.11g и коммутатором Ethernet

Руководство пользователя

Версия 3.6
2/2009
Редакция 1

ZyXEL

О данном руководстве пользователя

Для кого предназначено данное руководство

Данное руководство предназначено для тех, кто планирует производить настройку NBG334W с помощью Web-конфигуратора. Для работы с руководством необходимо обладать основными знаниями о топологии и принципах организации сетей TCP/IP.

Зарегистрируйте ваше изделие ZyXEL через Интернет по адресу *zyxel.ru* для России, *ua.zyxel.com* – для Украины и *zyxel.kz* – для Казахстана. Регистрация изделия дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ и льгот.

Сопроводительная документация

- Краткое руководство

  Краткое руководство разработано с целью помочь Вам изучить устройство и начать работать с ним. В нем содержится информация о настройке сети и организации доступа в Интернет.
- Встроенная справка Web-конфигуратора

  Встроенная web-справка содержит описания отдельных окон и дополнительную информацию.

Рекомендуется выполнять настройку NBG334W с помощью содержащейся на прилагаемом диске программы ZyXEL NetFriend.

- Справочный компакт-диск

  Входящий в комплект компакт-диск содержит техническую документацию.
- Web-сайт корпорации ZyXEL
- Сертификаты на изделие, а также дополнительную документацию см. на сайте *zyxel.ru*.

Обратная связь с пользователями

Помогите нам помочь вам. Все комментарии, относящиеся к Руководству пользователя, вопросы и предложения по улучшению направляйте нам через Интерактивную систему консультаций в разделе «Поддержка» на сайте *zyxel.ru*. Спасибо.

Обозначения, принятые в документе

Предупреждения и примечания

Предупреждения и примечания в данном руководстве пользователя представлены следующим образом:

Значком «предупреждение» отмечены пункты, содержание которых предупреждает о возможном нанесении вреда пользователю или устройству.

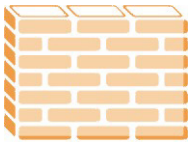
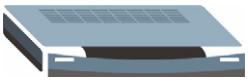
Значком «примечание» помечается важная информация (например, необходимость настройки других параметров или полезные подсказки), рекомендации, относящиеся к теме.

Условные обозначения

- Далее в данном руководстве интернет-центр NBG334W может именоваться как «устройство», «изделие» или «система» NBG334W.
- Надписи на изделии, имена окон, имена полей и пункты меню обозначаются **жирным** шрифтом.
- Названия клавиш указаны прописными буквами в квадратных скобках, например, [ENTER] означает клавишу «ввод» или «возврат каретки» на клавиатуре.
- Указание «Введите...» означает, что следует набрать один или несколько символов и затем нажать клавишу [ENTER]. «Выберите» означает, что следует использовать один из предложенных вариантов.
- Правая угловая скобка (>) между названиями окон означает нажатие кнопки мыши. Например, **Maintenance (Сопровождение) > Log (Регистрационный журнал) > Log Setting (Настройки регистрационного журнала)** означает, что сначала необходимо выбрать **Maintenance (Сопровождение)** в панели навигации, затем подменю **Log (Регистрационный журнал)**, а затем закладку **Log Setting (Настройки регистрационного журнала)**.
- Единицы измерения могут указывать как на «метрические», так и на «научные» величины. Например, приставка «к» (кило) может означать как 1000, так и 1024, приставка «М» – 1000000 или 1048576 и т. д.
- «напр.» – это сокращение для «например», а «т. е.» – для «то есть».

Используемые пиктограммы

В схемах данного руководства используются приведенные ниже пиктограммы. Значок NBG334W является схематичным изображением устройства.

NBG334W	Компьютер	Ноутбук
Сервер	Концентратор DSLAM	Межсетевой экран 
Телефон	Коммутатор	Маршрутизатор
Модем 		

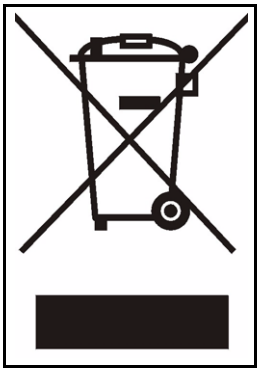
Техника безопасности

Для обеспечения безопасности необходимо ознакомиться со следующими правилами и следовать им.

- Не используйте изделие в непосредственной близости от воды, например, во влажных подвалах или рядом с бассейном.
- Не подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- Не кладите на устройство какие-либо посторонние предметы.
- ЗАПРЕЩАЕТСЯ устанавливать, использовать и ремонтировать устройство во время грозы. Существует определенный риск получения удара электрическим током при разряде молнии.
- Подключайте к устройству ТОЛЬКО соответствующие комплектующие.
- Не вскрывайте устройство. Не следует открывать или снимать крышку во избежание поражения электрическим током высокого напряжения и других повреждений. Техническое обслуживание и разборка данного устройства должны выполняться только квалифицированным техническим персоналом. Пожалуйста, свяжитесь с местным поставщиком для получения информации о техническом обслуживании.
- Убедитесь, что все кабели подключены к соответствующим портам.
- Прокладывайте соединительные кабели в местах, где никто не будет наступать на них или спотыкаться.
- Всегда отсоединяйте от устройства все кабели перед обслуживанием или разборкой.
- Используйте для устройства ТОЛЬКО соответствующий адаптер питания.
- Подключите адаптер питания к сети электропитания с соответствующим напряжением (110 В переменного тока в Северной Америке или 230 В переменного тока в Европе).
- Не кладите на адаптер питания какие-либо предметы и не располагайте его в местах, где могут ходить люди.
- Не используйте устройство, если адаптер питания неисправен, так как это может привести к поражению электрическим током.
- Если адаптер питания поврежден, отключите его от розетки электропитания.
- Не пытайтесь ремонтировать адаптер питания. Для заказа нового адаптера питания свяжитесь с местным поставщиком.
- Не используйте устройство вне помещения и убедитесь, что все соединения также находятся внутри помещения. Существует определенный риск получения удара электрическим током при разряде молнии.
- Не заслоняйте вентиляционные отверстия устройства, так как недостаточный приток воздуха может стать причиной повреждения устройства.

- Внимание, антенна! Данное устройство соответствует требованиям сертификации ETSI и FCC при использовании с входящей в комплект антенной/антеннами. Используйте только входящую в комплект антенну/антенны.
- При настенной установке устройства убедитесь, что при монтаже не будут повреждены электропроводка, газо- или водопроводы.

Материалы изделия пригодны для переработки. Утилизация должна производиться надлежащим образом.



Содержание

Введение **11**

Знакомство с интернет-центром NBG334W 13
Знакомство с Web-конфигуратором 17
Учебное руководство по развертыванию беспроводной сети 31

Сеть **37**

Беспроводная локальная сеть (WLAN) 39
WAN 63
LAN 77
DHCP 83
Трансляция сетевых адресов (NAT) 89
Динамическая система доменных имен 99

Безопасность **103**

Межсетевой экран 105
Фильтрация на основе содержания 113

Управление **119**

Окна настройки статических маршрутов 121
Управление пропускной способностью 125
Удаленное управление 139
Универсальная функция Plug and Play (UPnP) 145

Обслуживание, поиск и устранение неисправностей **157**

Система 159
Регистрационные журналы 165
Программные средства 183
Поиск и устранение неисправностей 189

Приложения и алфавитный указатель **197**

Часть I
Введение

Знакомство с интернет-центром NBG334W (13)
Учебное руководство по развертыванию беспроводной сети (31)
Знакомство с Web-конфигуратором (17)

1

Знакомство с интернет-центром NBG334W

В этой главе рассказывается об основных функциях и сферах применения NBG334W.

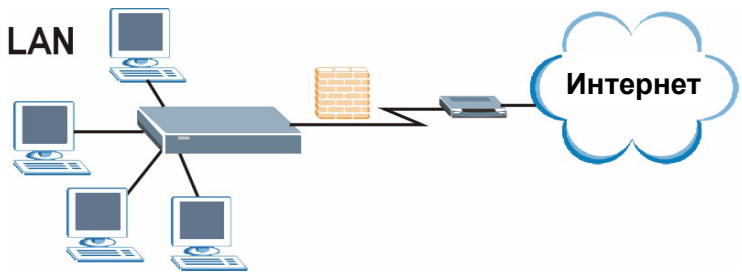
1.1 Обзор

Интернет-центр NBG334W – это беспроводной маршрутизатор с функцией межсетевого экрана, контролирующего обмен данными между сетью Интернет и локальной сетью.

1.1.1 Защищенный широкополосный доступ в сеть Интернет

К интернет-центру NBG334W можно подключить выделенную линию Ethernet для обеспечения общего доступа в сеть Интернет с использованием функций межсетевого экрана и фильтрации содержимого. Для более эффективного управления трафиком сети интернет-центр оснащен функцией управления полосой пропускания. Функция обеспечения качества обслуживания (QoS) позволяет предоставлять приоритет критичным по времени или особо важным приложениям, например, программам для передачи голоса по сети Интернет (VoIP).

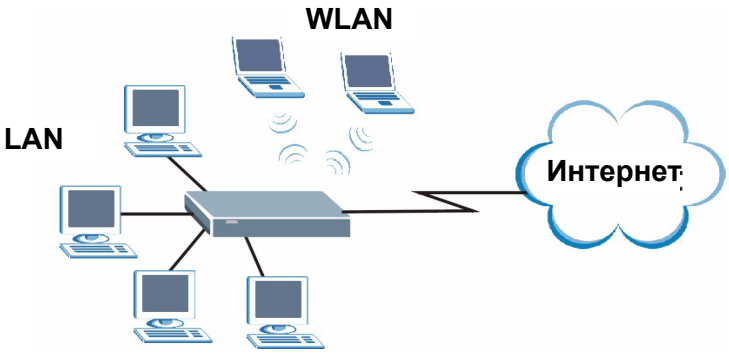
Рис. 1 Защищенный доступ в сеть Интернет



1.1.2 Организация беспроводной локальной сети

Функция беспроводной локальной сети интернет-центра NBG334W предоставляет беспроводным клиентам, поддерживающим стандарт IEEE 802.11b или IEEE 802.11g, возможность доступа в сеть Интернет или в локальную сеть, а также возможность взаимодействия между собой. При этом беспроводные станции можно свободно перемещать в зоне покрытия, сохраняя доступ к ресурсам проводной сети.

Рис. 2 Пример организации беспроводной локальной сети (WLAN)



1.2 Способы управления интернет-центром NBG334W

Для управления интернет-центром NBG334W используются следующие средства:

- Web-конфигуратор. Рекомендуется для повседневного управления интернет-центром NBG334W с использованием рекомендуемого Web-браузера.
- Интерфейс командной строки. Управление с помощью команд главным образом используется сервисными инженерами при поиске и устранении неисправностей.
- FTP. Протокол FTP (File Transfer Protocol – протокол передачи файлов) используется для обновления микропрограммы и резервного сохранения/восстановления конфигурации.

1.3 Полезные советы по управлению интернет-центром NBG334W

Для обеспечения безопасности и более эффективной работы интернет-центра NBG334W рекомендуется регулярно выполнять нижеприведенные инструкции для интернет-центра NBG334W.

- Изменение пароля. Необходимо использовать пароль, который не поддается легкому угадыванию и состоит из символов различных типов, например, из букв и цифр.
- Запишите пароль и храните в безопасном месте.
- Сделайте резервное сохранение конфигурации (необходимо знать как выполнить восстановление конфигурации). В случае, если интернет-центр работает нестабильно или не работает вообще, может помочь восстановление предыдущей рабочей конфигурации. Если пароль утерян, необходимо выполнить сброс параметров NBG334W к настройкам, установленным изготовителем по умолчанию. При наличии файла предыдущей рабочей конфигурации не придется заново выполнять полную настройку NBG334W. Можно просто восстановить последнюю конфигурацию.

1.4 Светодиоды

Рис. 3 Передняя панель

Описание светодиодов представлено в следующей таблице.

Табл. 1 Светодиоды передней панели

СВЕТОДИОД	ЗНАЧОК	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER (ПИТАНИЕ)		Зеленый	Горит	Питание подается и NBG334W работает нормально.
			Не горит	Питание на NBG334W не подается.
LAN 1-4	1 2 3 4	Зеленый	Горит	Интернет-центр NBG334W успешно установил подключение Ethernet на скорости 10 Мбит/с.
			Мигает	NBG334W передает/принимает данные.
		Желтый	Горит	Интернет-центр NBG334W успешно установил подключение Ethernet на скорости 100 Мбит/с.
			Мигает	NBG334W передает/принимает данные.
			Не горит	Локальная сеть не подключена.
WAN		Зеленый	Горит	Интернет-центр NBG334W успешно установил подключение WAN на скорости 10 Мбит/с.
			Мигает	NBG334W передает/принимает данные.
		Желтый	Горит	Интернет-центр NBG334W успешно установил подключение Ethernet на скорости 100 Мбит/с.
			Мигает	NBG334W передает/принимает данные.
		Нет	Не горит	Подключение WAN не готово или не установлено.
WLAN		Зеленый	Горит	Интернет-центр NBG334W готов, но не передает и не принимает данные по беспроводной сети.
			Мигает	Интернет-центр NBG334W принимает/передает данные по беспроводной сети.
		Нет	Не горит	Беспроводная сеть не готова или неисправна.
WPS		Защита беспроводной сети Wi-Fi.		

2

Знакомство с Web-конфигуратором

В этой главе описывается доступ к web-конфигуратору NBG334W и приводится обзор его окон.

2.1 Описание Web-конфигуратора

Web-конфигуратор – это интерфейс управления на основе технологии HTML, который позволяет выполнять настройку и управление интернет-центром NBG334W с помощью браузера Интернет. Следует использовать Internet Explorer версии 6.0 и выше либо Netscape Navigator версии 7.0 и выше. Рекомендуемое разрешение экрана: 1024 на 768 пикселей.

Чтобы воспользоваться web-конфигуратором, необходимо включить следующие параметры:

- Инициированные интернет-центром всплывающие окна в Интернет-браузере. Блокировка всплывающих окон активирована по умолчанию в Windows XP SP2.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

Информацию о том, как проверить, действительно ли эти функции включены в браузере Internet Explorer, см. в главе «Поиск и устранение неисправностей».

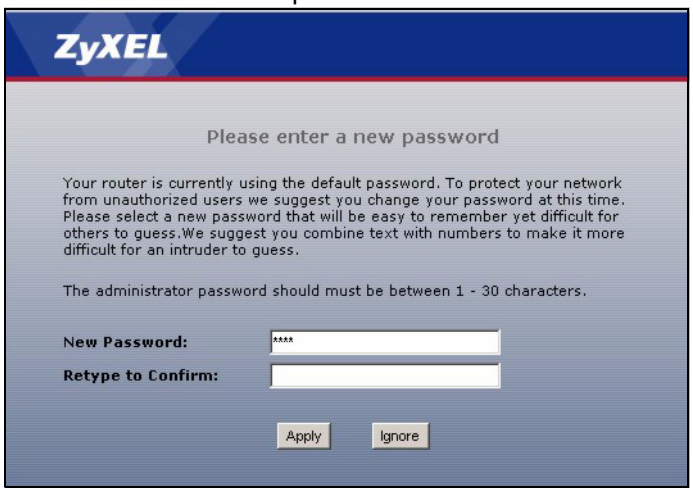
2.2 Доступ к Web-конфигуратору

1. Убедитесь, что интернет-центр NBG334W подключен правильно и подготовьте компьютер/компьютерную сеть к подключению NBG334W (см. Краткое руководство).
2. Запустите Web-браузер.
3. В строке адреса введите "http://192.168.1.1".

4 Введите в качестве пароля «1234» (по умолчанию) и нажмите кнопку **Login (Вход в систему)**. В некоторых версиях пароль по умолчанию появляется автоматически. В этом случае просто нажмите кнопку **Login (Вход в систему)**.

5 В результате должно открыться окно с предложением о смене пароля, которое рекомендуется принять (см. рисунок). Введите новый пароль и подтвердите его, затем нажмите кнопку **Apply (Применить)** или **Ignore (Пропустить)**.

Рис. 4 Окно смены пароля



Сеанс управления будет автоматически завершен по истечении периода времени, установленного в поле **Administrator Inactivity Timer (Время простоя в режиме администрирования)**, по умолчанию – 5 минут. В этом случае следует снова выполнить процедуру регистрации в NBG334W.

2.3 Сброс настроек интернет-центра NBG334W к заводским установкам

Если вы забыли пароль или не можете получить доступ к Web-конфигуратору, необходимо нажать на кнопку **RESET** на задней панели NBG334W для загрузки файла конфигурации, установленного изготовителем по умолчанию. Это означает, что прежняя конфигурация будет полностью потеряна и пароль будет сброшен на значение по умолчанию «1234».

2.3.1 Пользование кнопкой Reset (Сброс)

1 Убедитесь, что горит светодиод **PWR**.

2 Нажмите и удерживайте кнопку **RESET (СБРОС)** в течение десяти секунд или до тех пор, пока светодиод **PWR** не начнет мигать, затем отпустите ее. Когда

светодиод **PWR** начинает мигать, это означает, что настройки по умолчанию восстановлены и происходит перезапуск NBG334W.

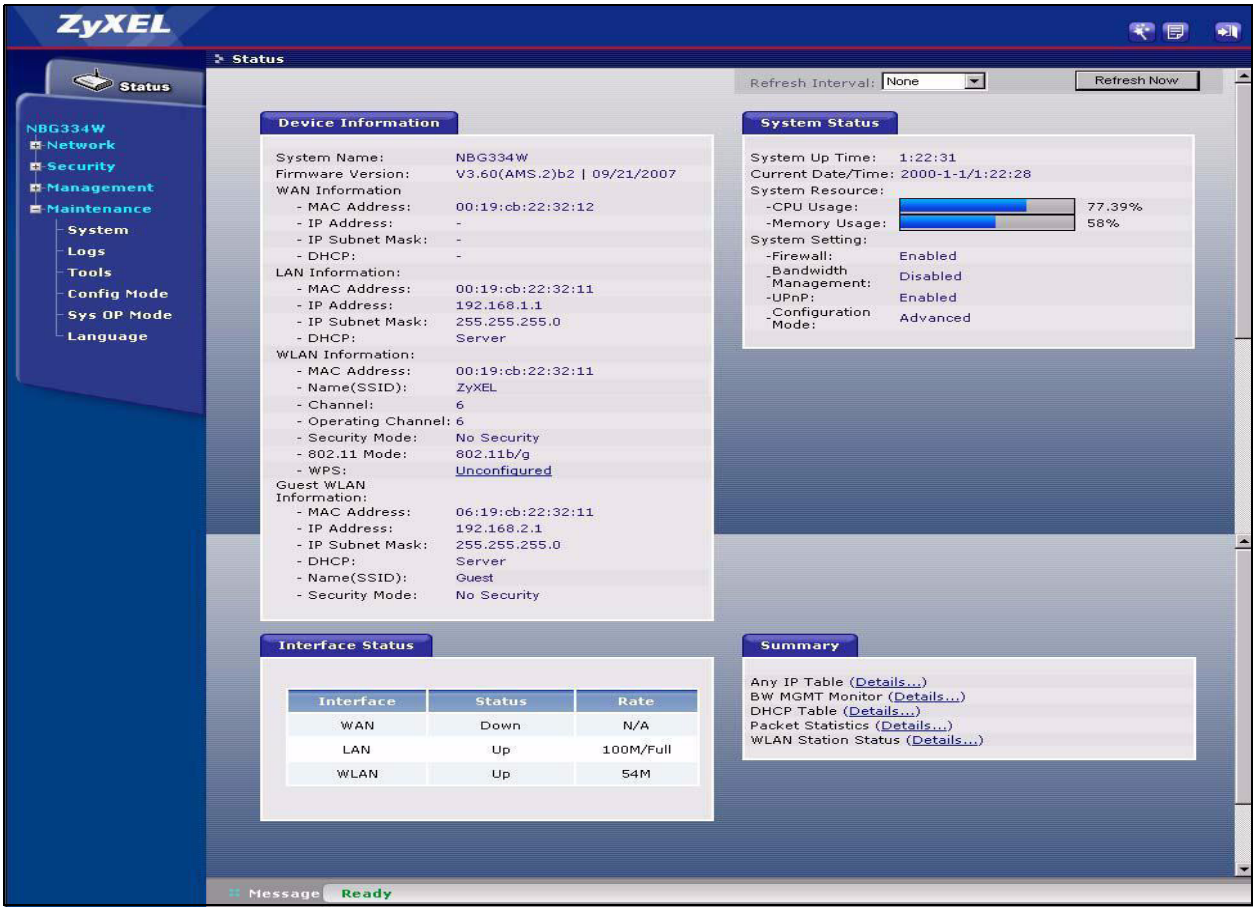
2.4 Интерфейс Web-конфигуратора

В этом разделе рассказывается, как работать с Web-конфигуратором из окна **Status (Состояние)**.

2.4.1 Окно Status (Состояние)

Следующее окно открывается при входе в NBG334W.

Рис. 5 Окно состояния Web-конфигуратора



В следующей таблице представлено описание значков окна **Status (Состояние)**.

Табл. 2 Значки окна состояния

ЗНАЧОК	ОПИСАНИЕ
	Показывает информацию об авторском праве и ссылку на связанную с продуктом информацию.
	Значок выхода из Web-конфигуратора.

Табл. 2 Значки окна состояния (продолжение)

ЗНАЧОК	ОПИСАНИЕ
	Из этого выпадающего списка можно выбрать количество секунд для автоматического обновления статистики в окнах по истечение заданного временного интервала или значение **None (Нет)**, чтобы статистика не обновлялась.
	Обновляет статистическую информацию в окне.

В следующей таблице представлено описание элементов окна **Status (Состояние)**.

Табл. 3 Окно состояния Web-конфигуратора

ПОЛЕ	ОПИСАНИЕ
Device Information (Информация об устройстве)	
System Name (Системное имя)	Здесь отображается **System Name (Системное имя)**, которое вводится в окне **Maintenance (Сопровождение) > System (Система) > General (Общие настройки)**. Это имя используется для идентификации устройства.
Firmware Version (Версия микропрограммы)	Здесь отображается версия и дата создания микропрограммы ZyNOS.ZyNOS – это сетевая операционная система, собственная разработка ZyXEL.
WAN Information (Параметры глобальной сети)	
- MAC Address (MAC-адрес)	Показывает MAC-адрес Ethernet-адаптера WAN вашего устройства.
- IP Address (IP-адрес)	Здесь отображается IP-адрес порта WAN.
- IP Subnet Mask (IP-Маска подсети)	Здесь отображается маска подсети порта WAN.
- DHCP	Здесь отображается роль порта WAN – **Client (Клиент)** или **None (Нет)**.
LAN Information (Параметры локальной сети)	
- MAC Address (MAC-адрес)	Показывает MAC-адрес Ethernet-адаптера порта LAN вашего устройства.
- IP Address (IP-адрес)	Здесь отображается IP-адрес порта LAN.
- IP Subnet Mask (IP-Маска подсети)	Здесь отображается маска подсети порта LAN.
- DHCP	Здесь отображается роль порта LAN – **Server (Сервер)** или **None (Нет)**.
WLAN Information (Информация о беспроводной ЛВС)	
- MAC Address (MAC-адрес)	Показывает MAC-адрес беспроводного адаптера вашего устройства.
- Name (SSID) (Название (SSID))	Это описательное имя, используемое для идентификации NBG334W в беспроводной локальной сети.
- Channel (Канал)	Номер канала, выбирается вручную.
- Operating Channel (Рабочий канал)	Текущий канал, используемый интернет-центром NBG334W в беспроводной локальной сети.
- Security Mode (Режим безопасности)	Показывает уровень безопасности беспроводной сети, выбранный для NBG334W.

Табл. 3 Окно состояния Web-конфигуратора (продолжение)

ПОЛЕ	ОПИСАНИЕ
- 802.11 Mode (Режим 802.11)	Показывает стандарт беспроводной связи.
System Status (Состояние системы)	
System Uptime (Время работы системы)	Здесь отображается время, истекшее с момента запуска NBG334W.
Current Date/Time (Текущая дата/время)	В этом поле отображается текущая дата и время NBG334W.
System Resource (Системные ресурсы)	
- CPU Usage (Загрузка центрального процессора)	Показывает текущий процент использования вычислительной мощности интернет-центра NBG334W. Приближение этого значения к 100% означает, что интернет-центр NBG334W работает в режиме полной нагрузки, и увеличить его производительность больше нельзя. Если некоторым приложениям недостаточно вычислительной мощности устройства, следует закрыть другие приложения (например, в режиме управления пропускной способностью).
- Memory Usage (Использование памяти)	Показывает процент использования динамической памяти интернет-центра NBG334W. Операционная система ZyNOS (ZyXEL Network Operating System) не использует динамическую память, т.о., она может использоваться для работы таких функций как NAT и межсетевой экран.
System Setting (Настройки системы)	
- Firewall (Межсетевой экран)	Показывает, задействован ли межсетевой экран.
- Bandwidth Management (Управление пропускной способностью)	Показывает, включено ли управление пропускной способностью.
- UPnP	Показывает, включен ли режим UPnP.
Interface Status (Состояние интерфейса)	
Interface (Интерфейс)	В этом поле отображаются типы портов NBG334W. Устройство оборудовано портами следующих типов: **WAN**, **LAN** и **WLAN**.
Status (Состояние)	Порты LAN и WAN в этом поле могут принимать значения **Down (Откл.)** или **Up (Вкл.)**. Для беспроводного порта WLAN здесь отображается состояние **Up (Вкл.)**, если порт WLAN включен или **Down (Откл.)**, если порт WLAN отключен.
Rate (Скорость передачи)	Для портов LAN в этом поле отображается их скорость, значение параметра дуплексной передачи или **N/A (Недоступно)** (при отсутствии линии). Для порта WAN здесь отображается скорость порта и режим передачи, если используется инкапсуляция Ethernet, **Idle (Ожидание)** – простой канала (ppp), **Dial (Установление соединения)** – выполняется вызов и **Drop (Завершение соединения)** – разрыв соединения, если используется инкапсуляция PPPoE или PPTP. При отсутствии линии в этом поле отображается значение **N/A (Недоступно)**. Для беспроводного порта WLAN здесь отображается максимальная скорость передачи, если порт WLAN включен или **N/A (Недоступно)**, если порт WLAN отключен.
Summary (Сводка)	
Any IP Table (Таблица Any IP)	В этом окне отображаются IP-адреса устройств, не входящих в подсеть интернет-центра NBG334W.

Табл. 3 Окно состояния Web-конфигуратора (продолжение)

ПОЛЕ	ОПИСАНИЕ
BW MGMT Monitor (Мониторинг управления пропускной способностью)	В этом окне содержится информация о распределении и использовании пропускной способности NBG334W.
DHCP Table (Таблица DHCP)	В этом окне отображается текущая информация о клиентах DHCP.
Packet Statistics (Статистика пакетов)	В этом окне отображается статус портов и статистика пакетов.
WLAN Station Status (Состояние беспроводной станции)	В этом окне отображается список беспроводных станций, подключенных к NBG334W.

2.4.2 Панель навигации

После ввода пароля настройка функций интернет-центра NBG334W выполняется посредством перемещения по подпунктам меню в панели навигации.

Описание подменю представлено в следующей таблице.

Табл. 4 Сводная таблица окон

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Status (Состояние)		В этом окне отображается общая информация о состоянии устройства, системы и интерфейсов NBG334W. Это окно открывает доступ к таблицам, содержащим сводную статистику системы.
Network (Сеть)		
Wireless LAN (Беспроводная локальная сеть)	General (Общая настройка)	Это окно используется для настройки беспроводной локальной сети.
	MAC Filter (Фильтр MAC-адресов)	Параметры в этом окне позволяют настроить NBG334W на блокирование доступа к конкретным устройствам или блокирование доступа этих устройств к NBG334W.
	Advanced (Дополни-тельно)	Это окно используется для расширенной настройки беспроводной связи.
	QoS (Качество услуг)	Это окно используется для настройки качества услуги Wi-Fi Multimedia (WMM QoS). Функция WMM QoS позволяет назначать приоритет беспроводному трафику в соответствии с требованиями к доставке со стороны отдельных служб.
WAN (Глобальная сеть)	Internet Connection (Интернет-подключение)	Это окно позволяет назначить IP-адрес устройства в глобальной сети, установить параметры Интернет-провайдера, определить серверы DNS и настроить MAC-адреса WAN.
	Advanced (Дополни-тельно)	Это окно позволяет настроить дополнительные параметры.
LAN (Локальная сеть)	IP (IP-адрес)	Это окно используется для настройки IP-адреса и маски подсети ЛВС.
	IP Alias (Псевдоним IP)	Это окно позволяет разделить локальную сеть на подсети.
	Advanced (Дополни-тельно)	Это окно позволяет включить настройку дополнительных параметров.
DHCP Server (Сервер DHCP)	General (Общая настройка)	Это окно позволяет задействовать сервер DHCP интернет-центра NBG334W.
	Advanced (Дополни-тельная настройка)	В этом окне можно назначить IP-адреса конкретным компьютерам, основываясь на их MAC-адресах и включить назначение DNS-серверов сервером DHCP.
	Client List (Список клиентов)	Это окно используется для просмотра параметров конкретного клиента DHCP и назначения IP-адреса по MAC-адресу (и имени узла).

Табл. 4 Сводная таблица окон

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
NAT (Трансляция сетевых адресов)	General (Общая настройка)	Это окно используется для включения функции NAT.
	Application (Приложение)	Это окно используется для настройки серверов, находящихся за NBG334W.
	Advanced (Дополнительная настройка)	Это окно используется для изменения настроек инициализации портов NBG334W.
DDNS (Динамическая система назначения доменных имен)	General (Общая настройка)	Это окно используется для настройки динамической службы DNS.
Security (Безопасность)		
Firewall (Межсетевой экран)	General (Общая настройка)	Это окно используется для включения или выключения межсетевого экрана.
	Services (Службы)	Это окно показывает список правил межсетевого экрана и позволяет редактировать/добавлять правила.
Content Filter (Контент-фильтр)	Filter (Фильтр)	Это окно позволяет включить блокировку конкретных веб-функций и сайтов, содержащих в URL-адресе заданные ключевые слова.
	Schedule (График)	В этом окне устанавливается расписание, по которому NBG334W выполняет фильтрацию содержания.
Management (Управление)		
Static Route (Статический маршрут)	IP Static Route (Статический маршрут IP)	Здесь выполняется настройка статических маршрутов IP.
Bandwidth MGMT (Управление пропускной способностью)	General (Общая настройка)	Это окно используется для включения режима управления пропускной способностью.
	Advanced (Дополнительная настройка)	Это окно используется для настройки пропускной способности восходящего соединения и редактирования правил управления пропускной способностью.
	Monitor (Мониторинг)	В этом окне содержится информация о распределении и использовании пропускной способности NBG334W.
Remote MGMT (Удаленное управление)	WWW (Всемирная паутина)	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление NBG334W по протоколу HTTP.
	Telnet (Сетевой теледоступ)	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление NBG334W по протоколу Telnet.
	FTP (Протокол передачи файлов)	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается доступ к NBG334W по протоколу FTP.
	DNS (Система доменных имен)	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователи могут посылать запросы DNS к NBG334W.

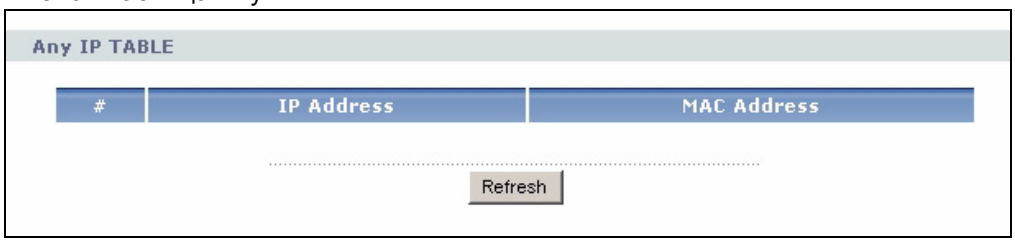
Табл. 4 Сводная таблица окон

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
UPnP (Универ-сальный режим Plug and Play)	General (Общая настройка)	Это окно используется для включения в NBG334W функции UPnP (универсальная функция Plug and Play).
Maintenance (Сопровождение)		
System (Система)	General (Общая настройка)	Это окно позволяет посмотреть и изменить параметры администрирования, например, доменное и системное имя, пароль и время простоя.
	Time Setting (Установка времени)	Это окно используется для изменения даты и времени в NBG334W.
Logs (Регистра-ционные журналы)	View Log (Просмотр журнала регистрации)	Это окно используется для просмотра журналов регистрации по выбранным категориям.
	Log Settings (Настройка журналов)	Это окно используется для изменения настроек регистрационных журналов NBG334W.
Tools (Сервисные программы)	Firmware (Микро-программа)	Это окно используется для загрузки микропрограммы в NBG334W.
	Configuration (Настройка)	Это окно позволяет выполнять резервное сохранение и восстановление конфигурации или сброс настроек NBG334W к заводским установкам.
	Restart (Перезапуск)	Это окно позволяет выполнить перезагрузку NBG334W без выключения электропитания.
Sys OP Mode (Режим работы системы)	General (Общая настройка)	Это окно позволяет выбрать режим работы

2.4.3 Сводка: Таблица IP-адресов

В этом окне отображаются IP-адреса всех компьютеров, использующих интернет-центр NBG334W посредством функции Any IP. Эта функция позволяет компьютерам выходить в Интернет через NBG334W без изменения своих сетевых настроек при включенной NAT. Чтобы открыть это окно, перейдите к окну **Status (Состояние)** (см. Разд. 2.4.1 на с. 19) и щелкните **Details... (Дополнительно...)** рядом с таблицей **Any IP Table (Таблица Any IP)**.

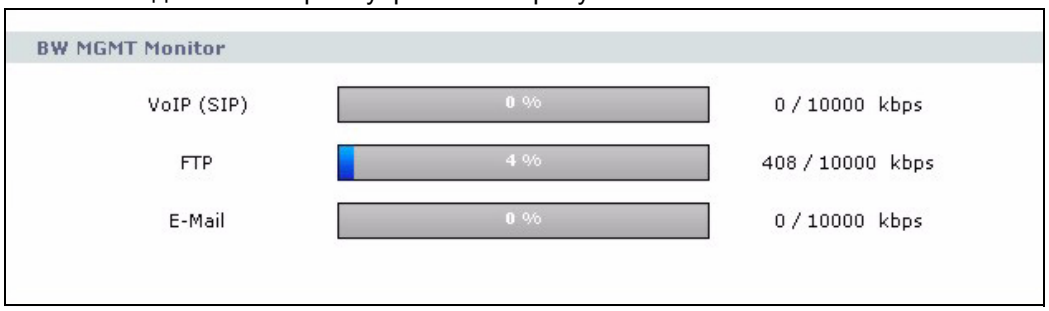
Рис. 6 Таблица Any IP



2.4.4 Сводка: Мониторинг управления пропускной способностью

В окне **Status (Состояние)** щелкните ссылку **BW MGMT Monitor (Details...) (Мониторинг управления пропускной способностью (Дополнительно...))**. Обратите внимание на использование пропускной способности правилами работы с WAN. Здесь также отображается использование пропускной способности относительно ее бюджета для каждого правила. Серая часть индикатора показывает неиспользуемую пропускную способность в процентах, а оранжевый цвет показывает используемую пропускную способность.

Рис. 7 Сводка: Мониторинг управления пропускной способностью

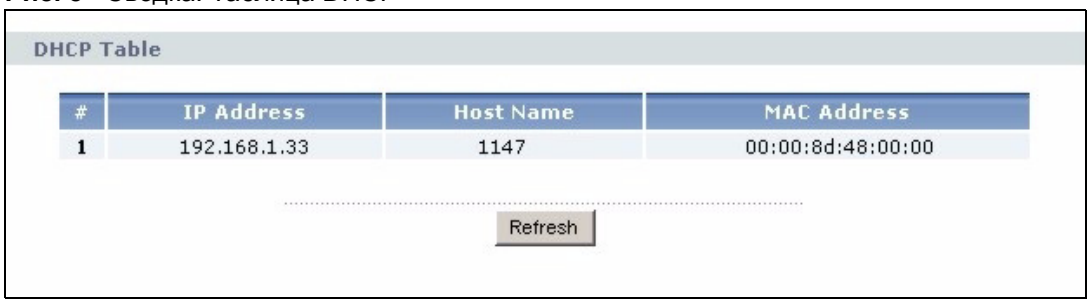


2.4.5 Сводка: Таблица DHCP

DHCP (Dynamic Host Configuration Protocol – Протокол динамической настройки узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать настройки TCP/IP при загрузке от центрального сервера DHCP. Можно настроить NBG334W как сервер DHCP или отключить эту функцию. При работе в режиме сервера NBG334W предоставляет клиентами DHCP конфигурацию TCP/IP. Если служба DHCP отключена, то для нормальной работы в локальной сети необходим другой сервер DHCP, в противном случае придется настраивать компьютер вручную.

В окне **Status (Состояние)** щелкните ссылку **DHCP Table (Details...) (Таблица DHCP (Дополнительно...))**. Появится окно с информацией о состоянии DHCP в режиме только для чтения. В таблице DHCP отображается текущая информация о клиентах DHCP (включая **IP-адрес**, **имя узла** и **MAC-адрес**) для всех клиентов сети, использующих NBG334W как сервер DHCP.

Рис. 8 Сводка: Таблица DHCP



В следующей таблице даны описания полей этого окна.

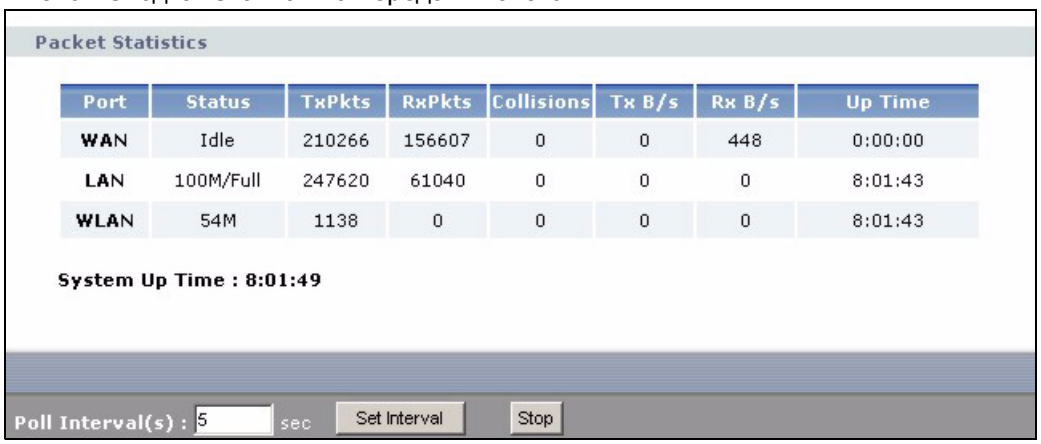
Табл. 5 Сводка: Таблица DHCP

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер узла.
IP Address (IP-адрес)	В этом поле отображается IP-адрес компьютера с номером, указанном выше.
Host Name (Имя узла)	В этом поле отображается имя компьютера.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес компьютера, чье имя указано в поле **Host Name (Имя узла)**. Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC – Media Access Control – Управление доступом к среде передачи). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.
Refresh (Обновить)	Нажмите **Refresh (Обновить)** для обновления окна.

2.4.6 Сводка: Статистика передачи пакетов

В окне **Status (Состояние)** щелкните ссылку **Packet Statistics (Details...) (Статистика передачи пакетов (Дополнительно...))**. Здесь отображается информация о состоянии портов и статистика пакетов в режиме только для чтения. Также здесь отображается время работы системы и интервалы опроса системы. Поле **Poll Interval(s) (Интервал опроса)** можно настраивать.

Рис. 9 Сводка: Статистика передачи пакетов



В следующей таблице даны описания полей этого окна.

Табл. 6 Сводка: Статистика передачи пакетов

ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Тип порта NBG334W.
Status (Состояние)	Для портов LAN в этом поле отображается их скорость, значение параметра дуплексной передачи или **Down (Откл.)** (при отсутствии линии). Для порта WAN здесь отображается скорость порта и режим передачи, если используется инкапсуляция Ethernet, **Idle (Ожидание)** – простой канала (ppp), **Dial (Установление соединения)** – выполняется вызов и **Drop (Завершение соединения)** – разрыв соединения, если используется инкапсуляция PPPoE или PPTP. При отсутствии линии в этом поле отображается значение **Down (Откл.)**. Для беспроводного порта WLAN здесь отображается максимальная скорость передачи, если порт WLAN включен или **Down (Откл.)**, если порт WLAN отключен.
TxPkts (Передано пакетов)	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, полученных через этот порт.
Collisions (Конфликты)	Здесь отображается количество конфликтов при передаче через данный порт.
Tx B/s (Скорость передачи, байт/с)	Здесь отображается скорость передачи порта в байтах в секунду.
Rx B/s (Скорость приема, байт/с)	Здесь отображается скорость приема порта в байтах в секунду.
Up Time (Время соединения)	Общее время подключения.

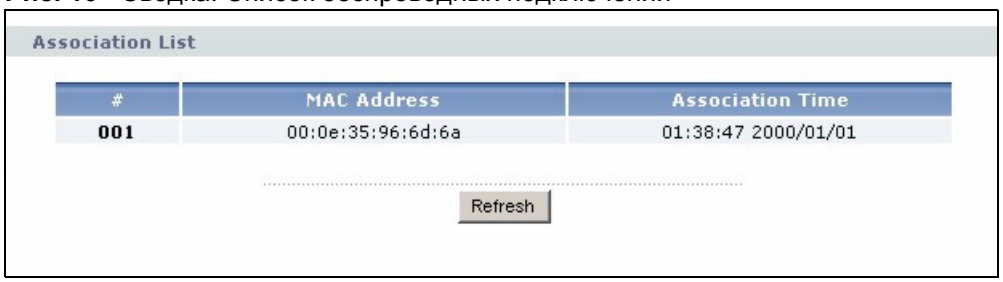
Табл. 6 Сводка: Статистика передачи пакетов

ПОЛЕ	ОПИСАНИЕ
System up Time (Время работы системы)	Здесь отображается время, истекшее с момента запуска NBG334W.
Poll Interval(s) (Интервал(ы) опроса)	В это поле вводится интервал обновления статистики.
Set Interval (Установить интервал)	Нажмите на эту кнопку, чтобы применить новый интервал опроса, заданный в поле **Poll Interval(s) (Интервал опроса)**.
Stop (Остановить)	Нажмите кнопку **Stop (Остановить)**, для остановки обновления статистики.

2.4.7 Сводка: Состояние беспроводных станций

Щелкните по ссылке **WLAN Station Status (Состояние беспроводных станций локальной сети)** в окне **Status (Состояние)**. В этом окне отображается список беспроводных станций, подключенных к NBG334W в окне **Association List (Список подключений)**.

Рис. 10 Сводка: Список беспроводных подключений



В следующей таблице даны описания полей этого окна.

Табл. 7 Сводка: Список беспроводных подключений

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер подключенного беспроводного устройства.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес подключенной беспроводной станции.
Association Time (Время подключения)	В этом поле отображается время, в течение которого беспроводная станция подключена к интернет-центру NBG334W.
Refresh (Обновить)	Нажмите **Refresh (Обновить)** для обновления окна.

3

Учебное руководство по развертыванию беспроводной сети

В этой главе на примерах рассматривается настройка взаимодействия точки доступа и беспроводного клиента с использованием нижеследующих параметров. Беспроводные клиенты могут выходить в сеть Интернет через точку доступа.

3.1 Пример параметров настройки

SSID (Идентификатор SSID)	SSID_Example3
Channel (Канал)	6
Security (Защита)	WPA-PSK (Pre-Shared Key (предварительно согласованный ключ): ThisismyWPA-PSKpre-sharedkey)
802.11 mode (Режим 802.11)	IEEE 802.11b/g

Далее в тексте точка доступа (AP: access point) или беспроводной маршрутизатор будет сокращенно обозначаться «AP», а компьютер с беспроводной сетевой картой или USB/PCI-адаптером – «беспроводным клиентом».

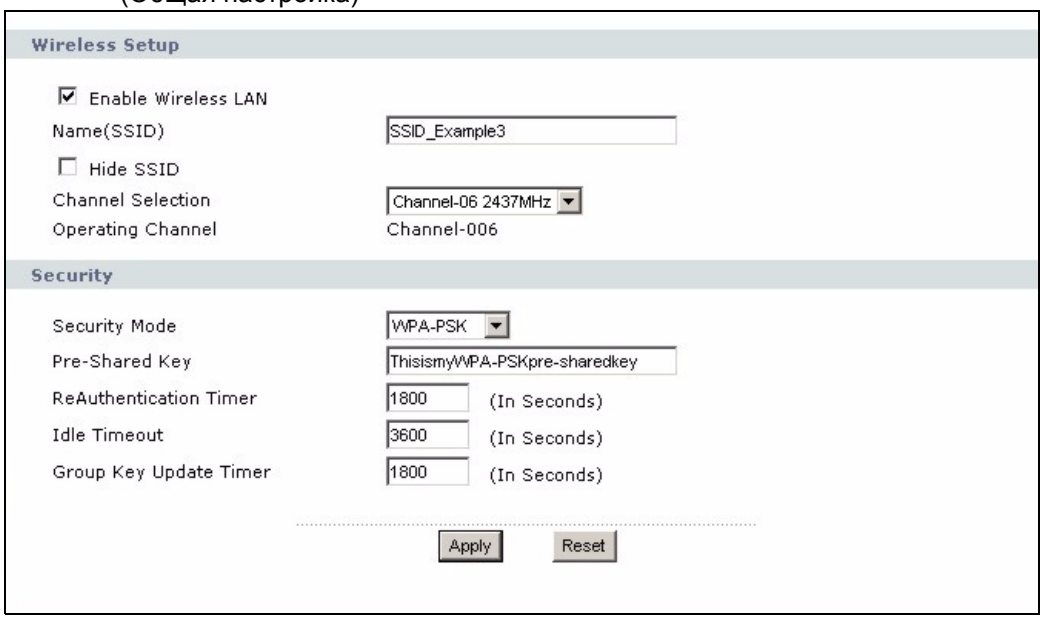
В следующих примерах приведены снимки окон сервисной программы настройки M-302 беспроводного клиента. Вид окон может незначительно отличаться у различных моделей.

3.2 Настройка точки доступа

Для настройки точки доступа следуйте нижеприведенной инструкции.

1 В веб-конфигураторе точки доступа откройте окно **Wireless LAN (Беспроводная локальная сеть) > General (Общая настройка)**.

Рис. 11 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > General (Общая настройка)



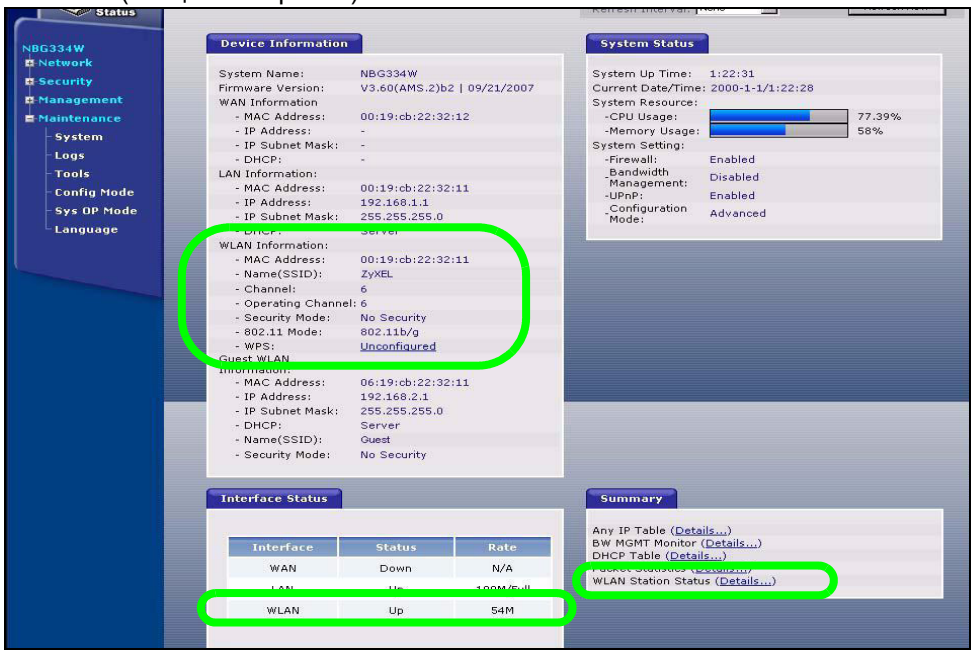
2 Установите флажок **Enable Wireless LAN (Включить беспроводную локальную сеть)**.

3 В качестве SSID введите «**SSID_Example3**» и выберите канал.

4 Выберите режим защиты **WPA-PSK** и введите **ThisismyWPA-PSKpre-sharedkey** в поле **Pre-Shared Key (Предварительно согласованный ключ)**. Нажмите кнопку **Apply (Применить)**.

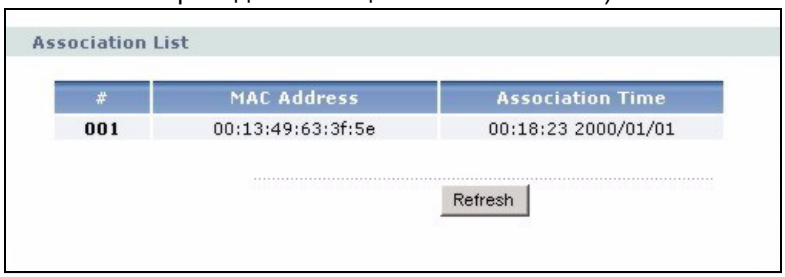
5 Откройте окно **Status (Состояние)**. Проверьте настройки беспроводной сети и безопасности в разделе **Device Information (Информация об устройстве)** и убедитесь, что в поле **Interface Status (Состояние интерфейса)** установлено значение **Up (Вкл.)**.

Рис. 12 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > General (Общая настройка)



6 Щелкните по ссылке **WLAN Station Status (Состояние беспроводной станции локальной сети)** в окне состояния точки доступа **(Status)**. В открывшемся окне можно наблюдать подключенных к точке доступа беспроводных клиентов.

Рис. 13 AP: Status: WLAN Station Status (Точка доступа: Состояние: Состояние беспроводной станции локальной сети)

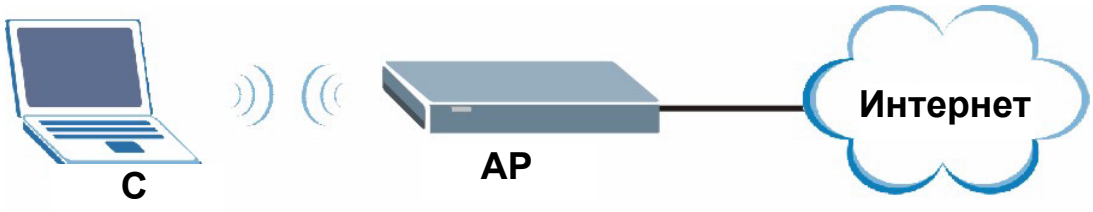


3.3 Настройка беспроводного клиента

В этом разделе пойдет речь о подключении к сети беспроводного клиента.

3.3.1 Подключение к беспроводной локальной сети

В следующих разделах описывается подключение к беспроводной сети, показанной на схеме ниже, с помощью утилиты беспроводного адаптера. На схеме беспроводной клиент обозначен буквой **C**, точка доступа – буквами **AP**.



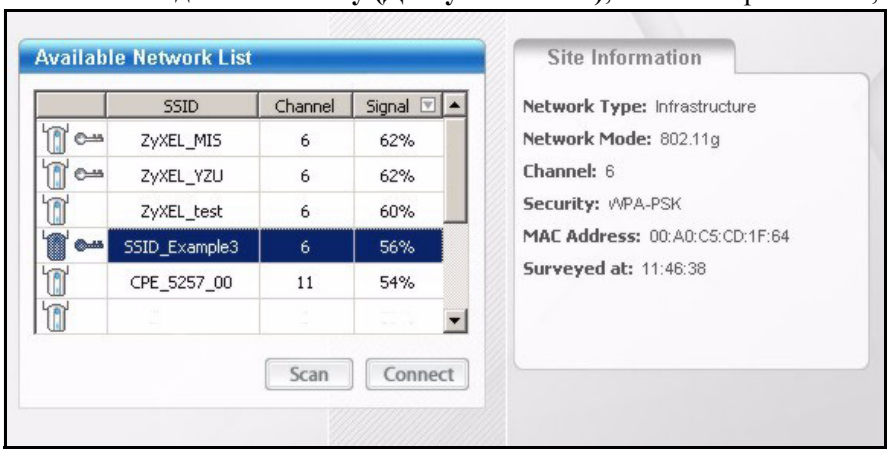
Существуют три способа подключения клиента к точке доступа.

- Не выполнять настройку и предоставить беспроводному клиенту произвести автоматический поиск и подключение к доступной сети, у которой не настроены параметры безопасности.
- Подключиться к беспроводной сети вручную.
- Настроить профиль беспроводного клиента для автоматического подключения к указанной сети или равноправному компьютеру.

В этом примере рассматривается подключение беспроводного клиента вручную к точке доступа с настроенной защитой WPA-PSK и выходом в Интернет. Для подключения к точке доступа необходимо знать ее идентификатор набора служб SSID и общий ключ WPA-PSK. В данном примере сетевым идентификатором (SSID) точки доступа является «SSID_Example3», а ключом сети – фраза «ThisismyWPA-PSKpre-sharedkey».

После установки утилиты беспроводного адаптера и беспроводного клиента выполните следующие действия для подключения к сети с помощью окна **Site Syrvey (Обзор узлов сети)**.

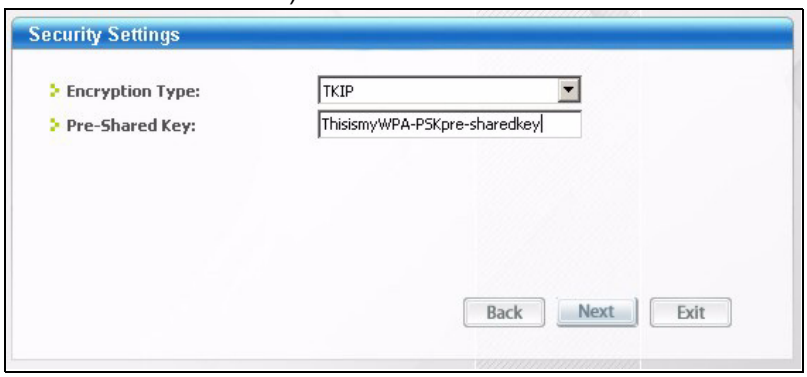
1 Запустите сервисную программу настройки беспроводного адаптера и щелкните по закладке **Site Survey (Доступные сети)**, чтобы открыть окно, показанное ниже.



2 Беспроводной клиент автоматически отыскивает доступные беспроводные сети. Нажмите кнопку **Scan (Поиск)**, если необходимо провести повторный поиск. Если в разделе **Available Network List (Список доступных сетей)** нет ни одной записи, значит, в зоне охвата адаптера нет доступных беспроводных сетей. Убедитесь, что точка доступа или равноправный компьютер включены, или разместите беспроводного клиента ближе к точке доступа или равноправному компьютеру.

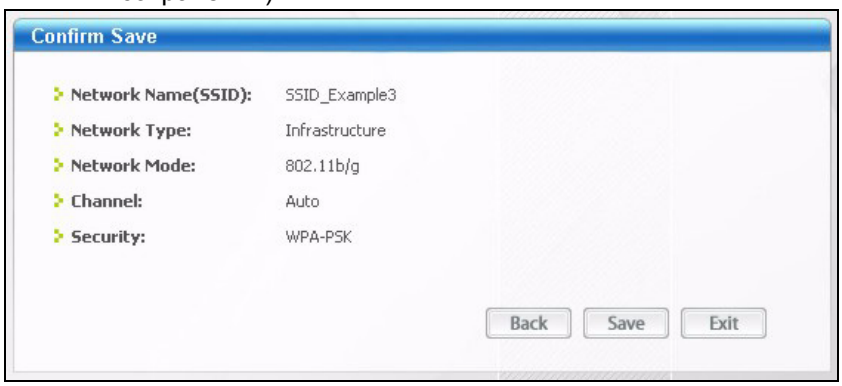
3 При попытке соединения с защищенной точкой доступа появится всплывающее окно с запросом на ввод параметров безопасности. Введите предварительно согласованный ключ, а в поле типа шифрования оставьте значение по умолчанию. Нажмите кнопку **Next (Далее)** для перехода к следующему окну. Для перехода к предыдущему окну нажмите кнопку **Back (Назад)**, для возврата в окно **Site Survey (Доступные сети)** нажмите кнопку **Exit (Выход)**.

Рис. 14 ZyXEL Utility: Security Settings (Сервисная программа ZyXEL: Параметры безопасности)



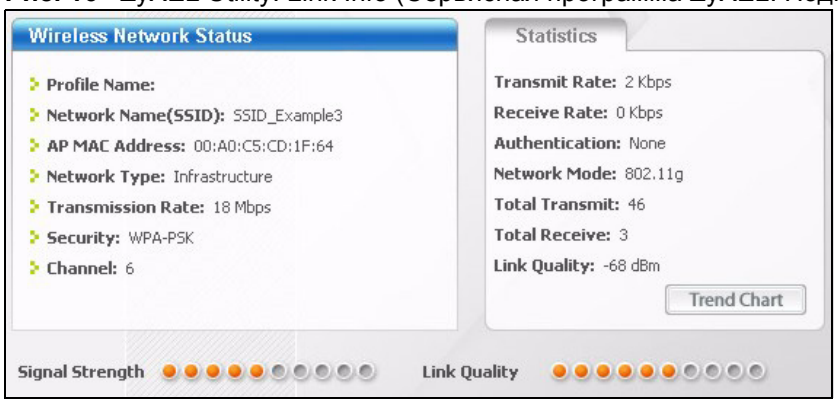
4 Появится окно **Confirm Save (Подтверждение новых настроек)**. Проверьте настройки и для продолжения нажмите **Save (Сохранить)**.

Рис. 15 ZyXEL Utility: Confirm Save (Сервисная программа ZyXEL: Подтверждение сохранения)



5 Во время соединения с беспроводной сетью с использованием заданных параметров сервисная программа настройки беспроводного адаптера отобразит окно **Link Info (Подключение)**. Когда канал беспроводной связи установится, значок сервисной программы настройки беспроводного адаптера на панели задач Windows станет зеленым, а в окне **Link Info (Подключение)** появится информация об активном соединении. Чтобы убедиться, что подключение к выбранной сети прошло успешно, проверьте информацию о сети в окне **Link Info (Подключение)**. Если беспроводной клиент не сможет подключиться к сети, поля этого окна останутся пустыми.

Рис. 16 ZyXEL Utility: Link Info (Сервисная программа ZyXEL: Подключение)



6 Откройте веб-обозреватель и введите в адресной строке http://zyxel.ru или адрес любого другого веб-сайта. Если сайт откроется, беспроводное соединение настроено успешно.

В противном случае следует изменить тип шифрования в окне **Security Settings (Параметры безопасности)**, просмотреть раздел «Поиск и устранение неисправностей» данного руководства или обратиться к администратору сети.

Часть II
Сеть

Беспроводная локальная сеть (WLAN) (39)
WAN (63)
LAN (77)
DHCP (83)
Трансляция сетевых адресов (NAT) (89)
Динамическая система доменных имен (99)

4

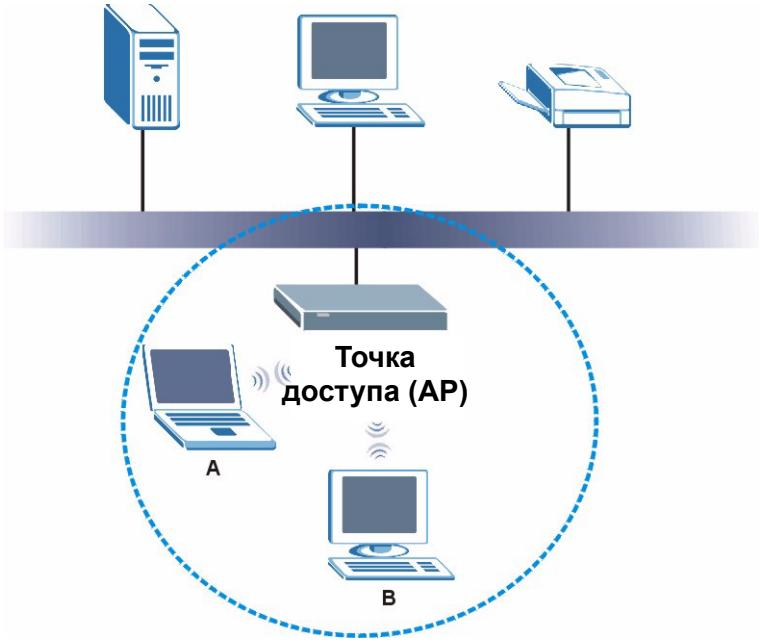
Беспроводная локальная сеть (WLAN)

В этой главе рассказывается, как настроить в NBG334W параметры беспроводной сети. Дополнительную информацию о беспроводных сетях см. в приложениях.

4.1 Обзор беспроводных сетей

На следующем рисунке представлен пример беспроводной сети.

Рис. 17 Пример беспроводной сети с точкой доступа



Беспроводная сеть обозначена синим кругом. Устройства A и B в этой сети называются беспроводными клиентами. Беспроводные клиенты используют точку доступа для подключения к другим устройствам (таким как принтер) или к сети Интернет. NBG334W является точкой доступа.

В любой беспроводной сети должны соблюдаться следующие принципы:

- Все беспроводные клиенты в одной беспроводной сети должны использовать одинаковый идентификатор SSID.

  SSID является именем беспроводной сети. SSID – это идентификатор набора служб (Service Set IDentity).
- Если зоны охвата двух беспроводных сетей перекрываются, необходимо, чтобы эти сети использовали разные каналы.

  Подобно радиостанциям или телевизионным каналам, беспроводные сети используют для приема и передачи информации определенные каналы или частоты.
- Все беспроводные устройства, находящиеся в одной беспроводной сети, должны использовать параметры безопасности, совместимые с точкой доступа.

  Настройка безопасности предотвращает доступ неавторизованных устройств к беспроводной сети. Кроме того, таким образом защищается передаваемая по сети информация.

Требования

Для расширения существующей локальной сети за счет организации беспроводной необходимы следующие элементы:

1. точка доступа (AP: access point) или маршрутизатор с функцией точки доступа
2. как минимум, одна беспроводная сетевая карта или адаптер, в зависимости от вашего компьютера.
   - При использовании настольного компьютера к нему можно подключить беспроводной USB- или PCI-адаптер.
   - При использовании ноутбука к нему можно подключить беспроводной USB- или CardBus-адаптер.
3. сервер RADIUS, если вы хотите использовать стандарт IEEE802.1x, WPA или WPA2

Для организации беспроводной сети без точки доступа или беспроводного маршрутизатора необходимы следующие элементы:

1. две или более беспроводных сетевых карты или адаптера, в зависимости от используемых компьютеров.
   - При использовании настольного компьютера к нему можно подключить беспроводной USB- или PCI-адаптер.
   - При использовании ноутбука к нему можно подключить беспроводной USB- или CardBus-адаптер.

Сведения для установки

Для организации беспроводной сети на основе точки доступа или беспроводного маршрутизатора следует на всех беспроводных устройствах прописать следующие параметры:

- SSID:_____
- Channel (Канал): auto (авто) или _____
- Network type of a wireless network card/adapter (тип сети беспроводной сетевой карты/адаптера): Infrastructure (с точкой доступа)
- wireless standard (стандарт беспроводной связи): IEEE 802.11b, g, b/g или a
- Security (безопасность):
  - ( ) None (нет)
  - ( ) WEP (64-, 128- или 256-битный ключ) (ASCII или Hex):_____
  - ( ) IEEE 802.1x
  - ( ) WPA-PSK (TKIP или AES):_____
  - ( ) WPA (TKIP или AES)
  - ( ) WPA2-PSK (TKIP или AES):_____
  - ( ) WPA2 (TKIP или AES)
- Preamble type (тип заголовка) (если используется): auto (авто), short (короткий) или long (длинный)

Для организации беспроводной сети без точки доступа или беспроводного маршрутизатора следует на всех беспроводных устройствах прописать следующие параметры:

- Network type (тип сети): Ad-Hoc (компьютер-компьютер)
- SSID:_____
- Channel (канал): _____
- wireless standard (стандарт беспроводной связи): IEEE 802.11b, g, b/g или a
- Security (безопасность):
  - ( ) None (нет)
  - ( ) WEP (64-, 128- или 256-битный ключ) (ASCII или Hex):_____

4.2 Защита беспроводной сети – общая информация

В следующих разделах представлены различные виды защиты, которые можно установить для беспроводной сети.

4.2.1 Идентификатор SSID

В стандартном режиме точка доступа работает как радиомаяк, регулярно транслируя в эфир идентификатор SSID. Можно скрыть SSID, и в этом случае точка доступа не будет транслировать SSID. Также можно изменить заданный по умолчанию SSID на трудноугадываемый идентификатор.

Однако этот метод не является достаточным для обеспечения безопасности беспроводной сети, поскольку существуют способы, при помощи которых неавторизованные беспроводные устройства могут получить SSID. Кроме того, неавторизованные беспроводные устройства могут получать информацию, передаваемую по беспроводной сети.

4.2.2 Фильтрация MAC-адресов

Каждый беспроводной клиент имеет уникальный идентификационный номер, называемый MAC-адрес.[1] Обычно MAC-адрес записывается двенадцатью шестнадцатеричными символами[2], например, 00A0C5000002 или 00:A0:C5:00:00:02. Информацию о MAC-адресе беспроводного клиента см. в руководстве пользователя или другой документации для конкретного устройства.

С помощью фильтра MAC-адресов в точке доступа можно назначить устройства, которым разрешено или не разрешено подключаться к данной беспроводной сети. Если беспроводному клиенту разрешено подключаться к беспроводной сети, ему все равно необходимо иметь правильные настройки (идентификатор SSID, номер канала и параметры безопасности). Если беспроводному клиенту не разрешено подключаться к беспроводной сети, то правильные настройки не имеют значения.

При использовании данного метода безопасности информация, передаваемая по беспроводной сети, не защищается. Более того, существуют способы, при помощи которых неавторизованные устройства могут получить MAC-адрес авторизованного клиента. Затем они могут использовать этот MAC-адрес для включения в беспроводную сеть.

4.2.3 Аутентификация пользователя

Перед подключением пользователя в беспроводную сеть его необходимо зарегистрировать. Этот процесс называется аутентификацией пользователя. Для прохождения аутентификации все беспроводные устройства в беспроводной сети должны поддерживать стандарт IEEE 802.1x.

1. Некоторые беспроводные устройства, например сканеры, могут определить наличие беспроводной сети, но не могут ее использовать. Такие устройства могут не иметь MAC-адреса.
2. Шестнадцатеричные символы: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

В беспроводных сетях имена пользователей и пароли для каждого пользователя обычно хранятся в двух местах.

- В точке доступа: такая функция называется базой данных локальных пользователей или локальной базой данных.
- На сервере RADIUS: такой сервер чаще используется на предприятиях, чем в жилых домах.

Если точка доступа не имеет базы данных локальных пользователей, и сервер RADIUS отсутствует, то невозможно устанавливать имена и пароли для пользователей.

Несанкционированные устройства могут получать информацию, передаваемую в беспроводной сети, даже если они не могут использовать эту беспроводную сеть. Более того, существуют способы получения несанкционированными беспроводными пользователями действующих имени пользователя и пароля. Затем они могут использовать это имя пользователя и пароль для подключения к беспроводной сети.

База данных локальных пользователей также имеет дополнительное ограничение, о котором рассказывается в следующем разделе.

4.2.4 Шифрование

Беспроводные сети могут использовать шифрование для защиты информации, передаваемой по беспроводной сети. Шифрование напоминает секретный код. Не зная кода нельзя прочесть сообщение.

Виды шифрования выбираются в зависимости от типа аутентификации пользователей. (Дополнительную информацию см. в Разд. 4.2.3 на с. 42.)

Табл. 8 Виды шифрования в зависимости от типа аутентификации

	АУТЕНТИФИКАЦИЯ ОТСУТСТВУЕТ	СЕРВЕР RADIUS
Самая слабая защита	Отключение защиты сети	WPA
	Статическое шифрование WEP	
	WPA-PSK	
Самая сильная защита	WPA2-PSK	WPA2

Например, если в беспроводной сети есть сервер RADIUS, можно использовать шифрование **WPA** или **WPA2**. Если пользователи не регистрируются в беспроводной сети, вы можете либо отключить шифрование, либо выбрать один из следующих типов шифрования: Статическое шифрование **WEP**, **WPA-PSK** или **WPA2-PSK**.

Обычно устанавливается самое сложное шифрование, которое поддерживает каждый клиент в беспроводной сети. Например, предположим, что точка доступа не имеет базы данных локальных пользователей, и сервер RADIUS также отсутствует. Следовательно, аутентификация пользователей отсутствует. Предположим также, что в беспроводной сети находится два беспроводных клиента. Устройство A поддерживает только шифрование WEP, а устройство B поддерживает WEP и WPA. Следовательно, в беспроводной сети следует установить **Static WEP (Статическое шифрование WEP)**.

В беспроводной сети рекомендуется использовать шифрование **WPA-PSK**, **WPA** или более сложное. Использование шифрования IEEE 802.1x и WEP все же лучше, чем полное отсутствие шифрования, но для несанкционированных устройств существует возможность достаточно быстро вычислить исходные данные для подключения.

При использовании локальной базы данных нельзя применить шифрование **WPA-PSK**, **WPA** или более сложное. В таком случае лучше установить более сложное шифрование без аутентификации, чем использовать простое шифрование вместе с локальной базой данных.

При выборе **WPA2** или **WPA2-PSK** в NBG334W можно также установить параметр **WPA compatible (Совместимость с WPA**) с целью реализации поддержки WPA. В таком случае, если одни беспроводные клиенты поддерживают WPA, а другие WPA2, необходимо установить **WPA2-PSK** или **WPA2** (в зависимости от типа регистрации в беспроводной сети), а также выбрать **WPA compatible (Совместимость с WPA)** в NBG334W.

В большинстве типов шифрования для защиты информации в беспроводной сети используется ключ. Чем длиннее ключ, тем сложнее шифрование. Все беспроводные клиенты в одной беспроводной сети должны использовать одинаковый ключ.

4.3 Роуминг

Беспроводной станцией называется устройство с беспроводным интерфейсом, совместимым со стандартом IEEE 802.11a/b/g. Мостом между проводной и беспроводной сетью служит точка доступа (AP: access point). Точка доступа создает область покрытия. Беспроводная станция может устанавливать соединение с точкой доступа только в этой зоне покрытия.

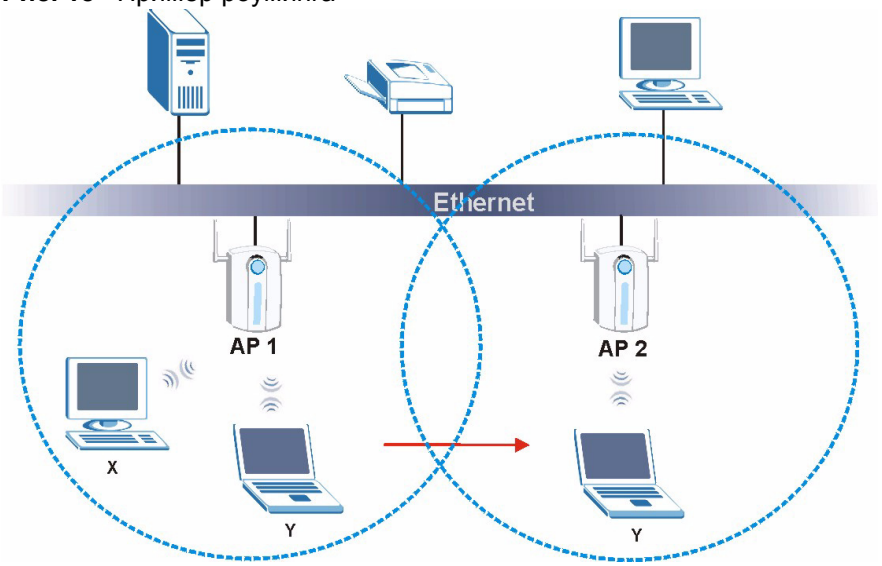
Если в сетевом окружении имеются несколько точек доступа, то беспроводные станции, перемещаясь между зонами их покрытия, могут переключаться с одной точки на другую. Такой процесс называется роумингом. Перемещаясь с места на место, беспроводная станция должна выбирать наиболее подходящую точку доступа, с точки зрения силы сигнала, нагрузки на сеть и других факторов.

Функция роуминга позволяет точкам доступа передавать между собой информацию о беспроводных станциях. Перемещаясь из одной зоны покрытия в другую, беспроводная станция находит канал новой точки доступа, после чего информирует остальные точки доступа локальной сети об этом изменении. Пример перемещения показан на рисунке Рис. 18 на с. 45.

Находясь в роуминге, подвижный пользователь беспроводной локальной сети не испытывает обрывов подключения к проводной сети через точку доступа.

Функция роуминга позволяет мостам обмениваться самой последней информацией обо всех беспроводных станциях, перемещающихся между точками доступа. Однако даже при отключенном роуминге беспроводные станции могут подключаться к другим точкам доступа. Включение этой функции гарантирует правильность перенаправления трафика (обновление таблиц мостов) и максимальную эффективность работы точки доступа. Точка доступа удаляет записи о беспроводных станциях, которые «привязываются» к другим точкам (сторонние точки доступа могут не иметь такой возможности). Обмен регистрационной информацией 802.1x не поддерживается (на момент написания данного руководства).

Рис. 18 Пример роуминга



Ниже пошагово описывается процесс роуминга.

1. Беспроводная станция **Y** перемещается из зоны покрытия точки доступа **AP 1** в зону покрытия точки **AP 2**.
2. Беспроводная станция **Y** находит сигнал точки **AP 2**.
3. Станция **Y** отправляет точке доступа **AP 2** запрос на привязку.
4. Точка доступа **AP 2** разрешает присутствие станции **Y** в своей зоне и передает информацию об этом точке доступа **AP 1** через проводную сеть.
5. Точка доступа **AP 1** регистрирует новое положение беспроводной станции **Y**.

4.3.1 Требования к роумингу

Для роуминга беспроводных станций между зонами покрытия должны выполняться следующие требования:

1. Все точки доступа должны входить в одну подсеть и иметь одинаковый идентификатор расширенного набора служб (ESSID).
2. Если на точке доступа включена локальная аутентификация пользователей по стандарту IEEE 802.1x, то новая точка доступа должна иметь профиль пользователя для беспроводной станции.
3. Соседние точки доступа, в случае пересечения их зон покрытия, должны использовать разные радио каналы.

4 Для передачи информации о роуминге все точки доступа должны использовать один номер порта.

5 Все точки доступа должны быть объединены в сеть Ethernet, а при использовании динамических IP-адресов, они должны быть способны получать эти адреса от сервера DHCP.

4.4 Качество услуги

В данном разделе описываются функции обеспечения качества обслуживания (QoS) интернет-центра NBG334W.

4.4.1 Качество предоставления услуг в беспроводной среде передачи

Функция WMM QoS (Wi-Fi MultiMedia – беспроводная среда передачи, Quality of Service – качество и класс предоставляемых услуг передачи данных) обеспечивает качество услуг в беспроводных сетях. Она контролирует приоритет передачи пакетов по беспроводной сети.

Беспроводной трафик получает приоритет на основе требований к срочности доставки. WMM QoS является расширением QoS в стандарте IEEE 802.11e для аттестованных беспроводных сетей.

Если функция WMM QoS отключена, всем потокам трафика предоставляется одинаковый приоритет для прохождения по беспроводной сети. Если при введении еще одного потока создаются требования, которые превышают текущую производительность сети, то из-за нового потока снижается пропускная способность сети для других потоков трафика.

С помощью функции WMM QoS интернет-центр NBG334W назначает приоритет потокам трафика в соответствии с признаками IEEE 802.1q или информацией DSCP, содержащейся в заголовках пакетов. Интернет-центр NBG334W автоматически определяет приоритетность пакетов, разделяя их по отдельным потокам трафика. Такой подход позволяет исключить задержки при передаче данных для приложений, чувствительных ко времени ожидания (задержкам) и колебаниям (вариациям) задержки.

4.4.1.1 Приоритеты WMM QoS

В следующей таблице описываются используемые интернет-центром NBG334W уровни приоритетности WMM QoS.

Табл. 9 Приоритеты WMM QoS

УРОВЕНЬ ПРИОРИТЕТНОСТИ	ОПИСАНИЕ
голос (WMM_VOICE)	Обычно применяется к трафику, особо чувствительному к колебаниям задержки. Используйте этот приоритет для сокращения задержек, чтобы повысить качество передачи голоса.
видео (WMM_VIDEO)	Обычно используется для трафика, который имеет некоторый допуск на колебание задержки, но требует приоритета над другими видами трафика данных.

Табл. 9 Приоритеты WMM QoS

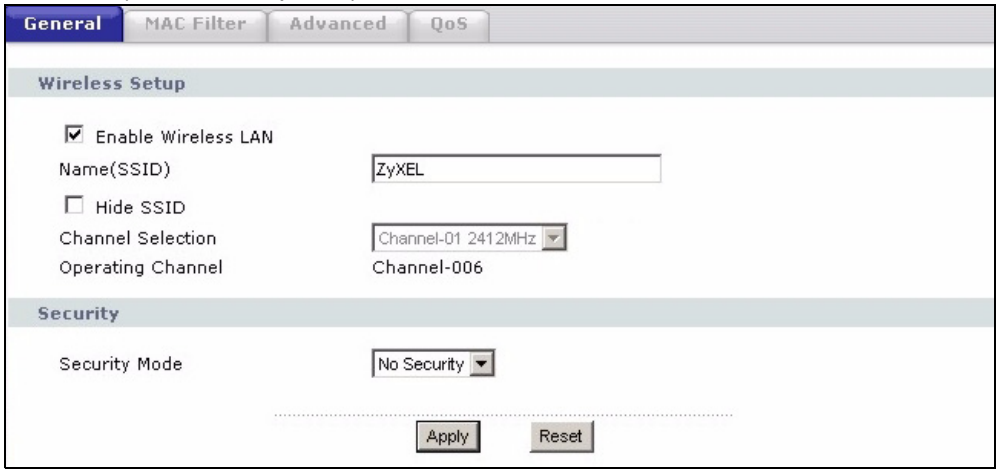
УРОВЕНЬ ПРИОРИТЕТНОСТИ	ОПИСАНИЕ
доставка методом наименьших затрат (WMM_BEST_EFFORT)	Обычно используется для трафика от приложений или устройств, которым требуются возможности QoS. Приоритет доставки методом наименьших затрат используется для трафика, который менее чувствителен ко времени ожидания, но не допускает больших задержек, как, например, Интернет-серфинг.
фоновая передача (WMM_BACKGROUND)	Обычно используется для некритического фонового трафика, как, например, групповая пересылка данных и задания на печать, которые допускают задержки и не влияют на другие приложения и пользователей. Приоритет фоновой передачи используется для приложений, которые не имеют жестких требований ко времени ожидания и пропускной способности.

4.5 Окно общих настроек беспроводной локальной сети

Если вы настраиваете NBG334W с компьютера, подключенного через беспроводную локальную сеть, и при этом изменяете в NBG334W идентификатор SSID, канал или настройки безопасности, то при нажатии на кнопку **Apply (Применить)** беспроводное соединение будет потеряно. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам NBG334W.

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть)**, чтобы открыть окно **General (Общие настройки)**.

Рис. 19 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > General (Общие настройки)



Приведенная ниже таблица описывает поля общих настроек беспроводной локальной сети.

Табл. 10 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > General (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN (Включить беспроводную локальную сеть)	Поставьте в этом поле флажок, чтобы включить беспроводную локальную сеть.
Name(SSID) (Название (SSID))	SSID (Service Set IDentity – Идентификатор набора служб) устанавливает набор служб для беспроводной станции. Беспроводные станции, подключенные к точке доступа (AP) должны иметь одинаковые идентификаторы SSID. Введите описательное имя для беспроводной локальной сети (не более 32 семиразрядных печатных символов ASCII).
Hide SSID (Скрыть SSID)	Поставьте флажок в этом поле, чтобы скрыть SSID в исходящем сигнальном кадре, в этом случае станция не сможет получить SSID при сканировании сети программами обзора узлов сети.
Channel Selection (Выбор канала)	Настройте рабочую частоту/канал в зависимости от Вашего региона. Выберите канал из раскрывающегося списка. Варианты выбора могут быть различными, в зависимости от используемой полосы частот (A или B/G) и страны нахождения.
Operating Channel (Рабочий канал)	В этом поле отображается радиоканал, который в данный момент использует интернет-центр NBG334W.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

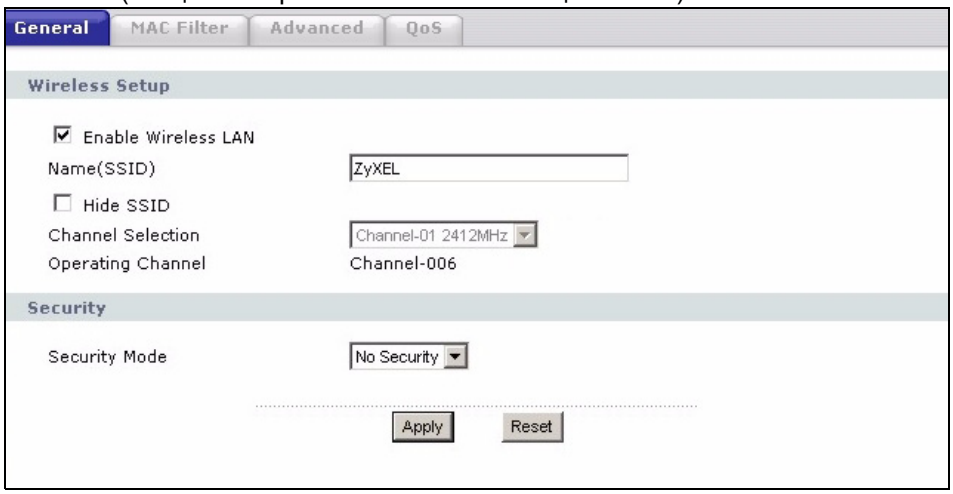
Описание других полей этого окна см. далее в этой главе.

4.5.1 Отключение защиты сети

Выберите **No Security (Отключить защиту)**, чтобы разрешить беспроводным станциям обмениваться данными с точками доступа без шифрования данных.

Если функция обеспечения беспроводной безопасности в NBG334W отключена, ваша сеть будет доступна для любого беспроводного сетевого устройства, которое находится в зоне охвата сети.

Рис. 20 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: No Security (Общие настройки: отключение защиты сети)



В следующей таблице даны описания полей этого окна.

Табл. 11 Беспроводное подключение: Отключение защиты

ПОЛЕ	ОПИСАНИЕ
Security Mode (Режим безопасности)	Из выпадающего списка выберите **No Security (Отключить защиту)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

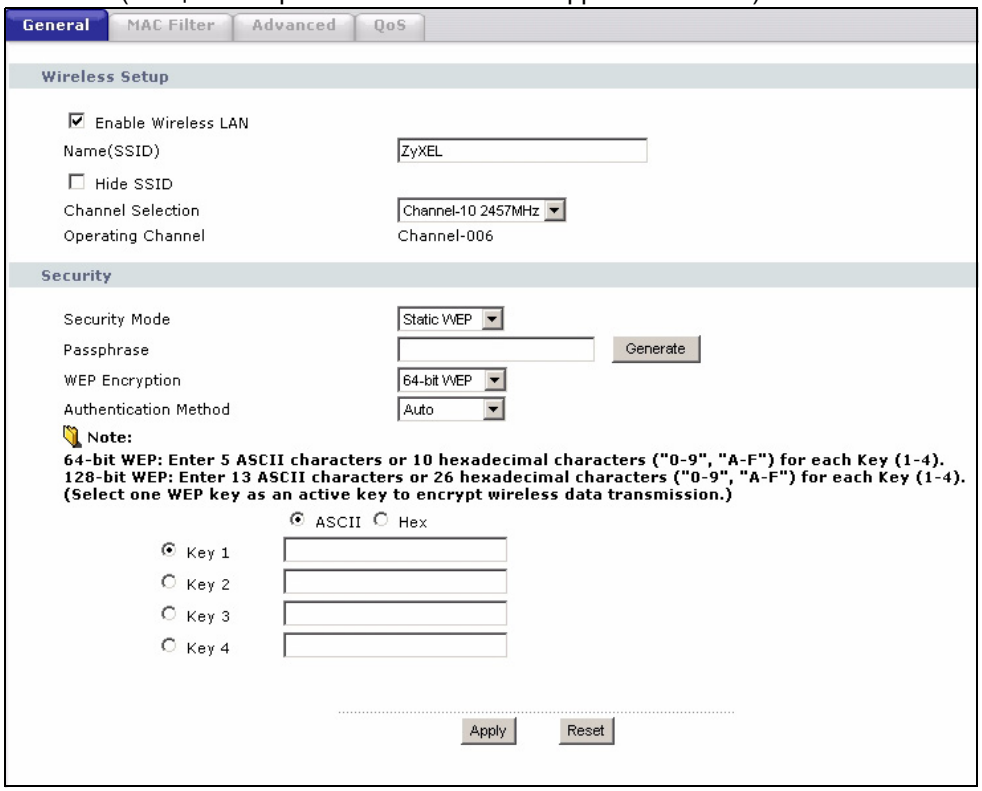
4.5.2 WEP-шифрование

WEP-шифрование кодирует передачу данных между беспроводными устройствами и точками доступа для предотвращения несанкционированного доступа. Шифруются передачи одноадресных и многоадресных рассылок в сети. Как беспроводные устройства, так и точки доступа должны использовать одинаковые ключи WEP.

NBG334W позволяет создать до четырех ключей WEP длиной 64 или 128 бит, но одновременно может использоваться только один ключ.

Чтобы включить и настроить шифрование WEP, щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть)** для отображения окна **General (Общие настройки)**. В списке **Security Mode (Режим безопасности)** выберите вариант **Static WEP (Статическое шифрование WEP)**.

Рис. 21 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: Static WEP (Общие настройки: статическое шифрование WEP)



В приведенной ниже таблице описываются поля для настройки безопасности беспроводной локальной сети.

Табл. 12 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: Static WEP (Общие настройки: статическое шифрование WEP)

ПОЛЕ	ОПИСАНИЕ
Passphrase (Ключевая фраза)	Введите идентификационную (парольную) фразу (до 32 печатных знаков) and щелкните **Generate (Генерировать)**. Интернет-центр NBG334W автоматически создаст четыре разных ключа WEP, которые будут отображены в полях **Key (Ключ)** ниже.
WEP Encryption (WEP-шифрование)	Выберите **64-bit WEP** или **128-bit WEP** для использования шифрования данных соответствующей разрядности.
Authentication Method (Метод аутенти-фикации)	Это поле активизируется при выборе в поле **WEP Encryption (Шифрование WEB)** варианта **«64-bit WEP»** или **«128-bit WEP»**. Из выпадающего списка выберите один из вариантов: **Auto (Автоматически)**, **Open System (Открытая система)** или **Shared Key (Общий ключ)**.
ASCII	Выберите этот вариант, чтобы в качестве ключа WEP ввести символы таблицы ASCII.
Hex (Шестна-дцатеричный)	Выберите этот вариант, чтобы в качестве ключа WEP ввести шестнадцатеричные символы. К ключу автоматически добавляется префикс «0x», который указывает на шестнадцатеричный ключ.

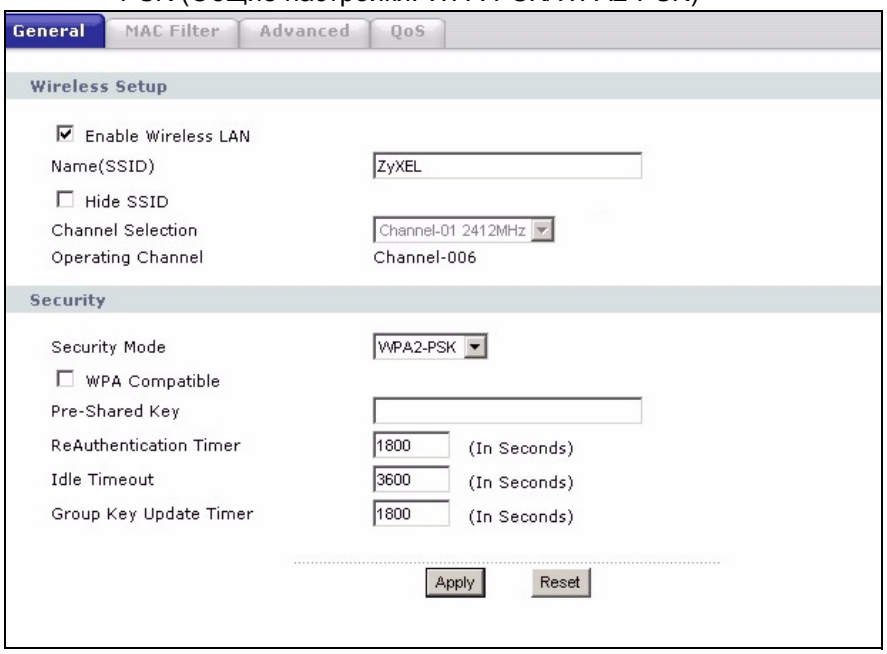
Табл. 12 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: Static WEP (Общие настройки: статическое шифрование WEP)

ПОЛЕ	ОПИСАНИЕ
Key 1 – Key 4 (Ключ 1 – Ключ 4)	Ключи WEP используются для шифрования данных. Для обеспечения передачи данных необходимо, чтобы NBG334W и все беспроводные станции использовали одинаковый ключ WEP. При выборе **64-bit WEP** нужно ввести 5 символов ASCII или 10 шестнадцатеричных символов («0-9», «A-F»). При выборе **128-bit WEP** нужно ввести 13 символов ASCII или 26 шестнадцатеричных символов («0-9», «A-F»). Настроить следует хотя бы один ключ, но одновременно активным может быть только один из них. По умолчанию активирован ключ 1.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

4.5.3 WPA-PSK/WPA2-PSK

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть)**, чтобы открыть окно **General (Общие настройки)**. Выберите вариант **«WPA-PSK»** или **«WPA2-PSK»** в списке **Security Mode (Режим безопасности)**.

Рис. 22 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: WPA-PSK/WPA2-PSK (Общие настройки: WPA-PSK/WPA2-PSK)



В следующей таблице даны описания полей этого окна.

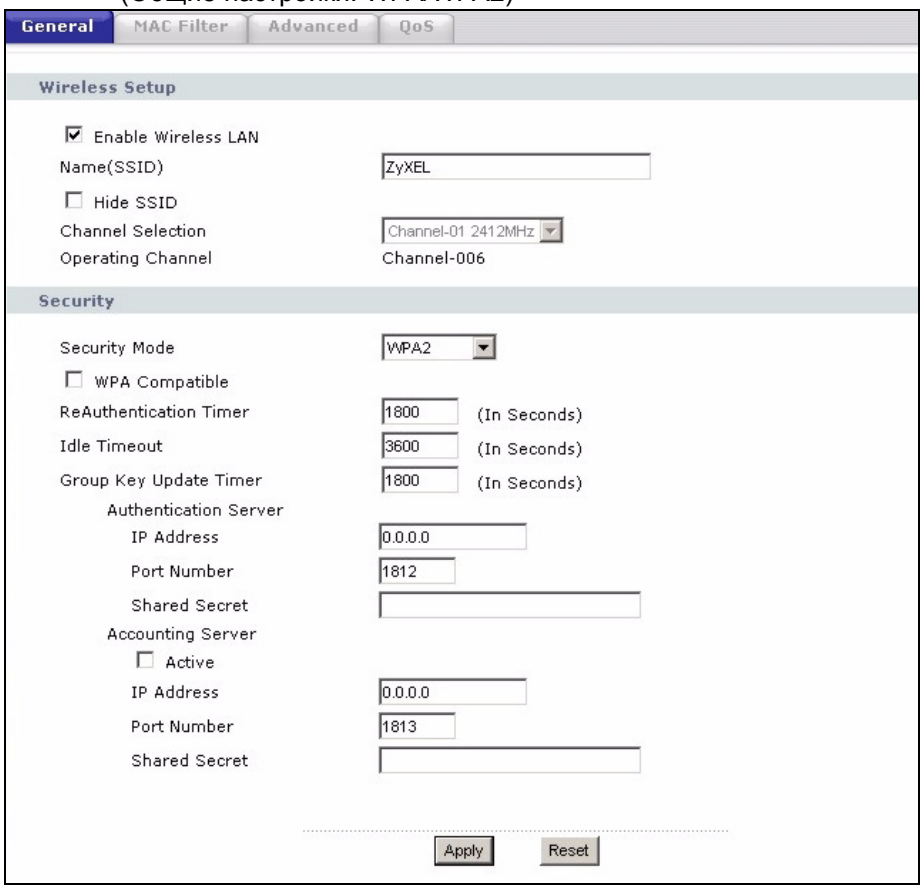
Табл. 13 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: WPA-PSK/WPA2-PSK (Общие настройки: WPA-PSK/WPA2-PSK)

ПОЛЕ	ОПИСАНИЕ
WPA Compatible (Совместимость с WPA)	Это поле доступно, только если в поле **Security Mode (Режим безопасности)** установлено **WPA2-PSK** или **WPA2**. Поставьте в этом поле флажок, чтобы клиенты WPA2 и WPA могли подключаться к NBG334W, даже если в NBG334W используется WPA2-PSK или WPA2.
Pre-Shared Key (Предварительно согласованный ключ)	Механизмы шифрования, используемые для **WPA/WPA2** и **WPA-PSK/WPA2-PSK**, являются одинаковыми. Разница между ними состоит в том, что при **WPA-PSK/WPA2-PSK** используется единственный общий ключ (пароль) для всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Введите предварительно согласованный ключ от 8 до 63 символов ASCII с учетом регистра (включая пробелы и знаки).
ReAuthentication Timer (Таймер повторной аутентификации (в секундах)	Установите интервал времени, через который беспроводные станции должны периодически передавать имя пользователя и пароль для того, чтобы оставаться в сети. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию – 1800 секунд (30 минут). Примечание: Если аутентификация беспроводного устройства производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.
Idle Timeout (Время простоя)	По истечении периода простоя NBG334W автоматически отключает беспроводное устройство от проводной сети. Для подключения к проводной сети беспроводное устройство должно снова отправить имя пользователя и пароль. По умолчанию устанавливается значение в 3600 секунд (или 1 час).
Group Key Update Timer (Таймер обновлений групповых ключей)	**Group Key Update Timer (Интервал обновления группового ключа)** – это интервал времени, через который точка доступа (если используется управление ключами **WPA-PSK/WPA2-PSK**) или сервер RADIUS (если используется управление ключами **WPA/WPA2**) передает новый групповой ключ всем клиентам. Процедура повторной настройки по ключу при WPA/WPA2 является эквивалентом автоматической периодической замены ключей WEP в точке доступа и всех устройствах беспроводной сети. Параметр **Group Key Update Timer (Интервал обновления группового ключа)** также поддерживается в режиме **WPA-PSK/WPA2-PSK**. По умолчанию устанавливается значение в **1800** секунд (30 минут).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

4.5.4 WPA/WPA2

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть)**, чтобы открыть окно **General (Общие настройки)**. Выберите **WPA** или **WPA2** в списке **Security Mode (Режим безопасности)**.

Рис. 23 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: WPA/WPA2 (Общие настройки: WPA/WPA2)



В следующей таблице даны описания полей этого окна.

Табл. 14 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: WPA/WPA2 (Общие настройки: WPA/WPA2)

ПОЛЕ	ОПИСАНИЕ
WPA Compatible (Совместимость с WPA)	Это поле доступно, только если в поле **Security Mode (Режим безопасности)** установлено **WPA2-PSK** или **WPA2**. Поставьте в этом поле флажок, чтобы клиенты WPA2 и WPA могли подключаться к NBG334W, даже если в NBG334W используется WPA2-PSK или WPA2.
ReAuthentication Timer (In Seconds) (Интервал повторной аутентификации (в секундах))	Установите интервал времени, через который беспроводные станции должны периодически передавать имя пользователя и пароль для того, чтобы оставаться в сети. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию – 1800 секунд (30 минут). Примечание: Если аутентификация беспроводного устройства производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.
Idle Timeout (Время простоя)	По истечении периода простоя NBG334W автоматически отключает беспроводное устройство от проводной сети. Для подключения к проводной сети беспроводное устройство должно снова отправить имя пользователя и пароль. По умолчанию устанавливается значение в 3600 секунд (или 1 час).
Group Key Update Timer (Таймер обновлений групповых ключей)	**Group Key Update Timer (Интервал обновления группового ключа)** – это интервал времени, через который точка доступа (если используется управление ключами **WPA-PSK/WPA2-PSK**) или сервер RADIUS (если используется управление ключами **WPA/WPA2**) передает новый групповой ключ всем клиентам. Процедура повторной настройки по ключу при WPA/WPA2 является эквивалентом автоматической периодической замены ключей WEP в точке доступа и всех устройствах беспроводной сети. Параметр **Group Key Update Timer (Интервал обновления группового ключа)** также поддерживается в режиме **WPA-PSK/WPA2-PSK**. По умолчанию в NBG334W устанавливается значение в **1800** секунд (30 минут).
Authentication Server (Сервер аутентификации)	
IP Address (IP-адрес)	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.
Port Number (Номер порта)	Введите номер порта сервера внешней аутентификации. Номер порта по умолчанию – **1812**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером аутентификации и NBG334W. Внешний сервер аутентификации и NBG334W должны использовать одинаковый ключ. Этот ключ не передается по сети.
Accounting Server (Сервер учета)	
Active (Активировать)	Выберите **Yes (Да)** из выпадающего списка для включения учета пользователей с помощью внешнего сервера аутентификации.
IP Address (IP-адрес)	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.
Port Number (Номер порта)	Введите номер порта внешнего сервера учета. Номер порта по умолчанию – **1813**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.

Табл. 14 Network (Сеть) > Wireless LAN (Беспроводная сеть) > General: WPA/WPA2 (Общие настройки: WPA/WPA2)

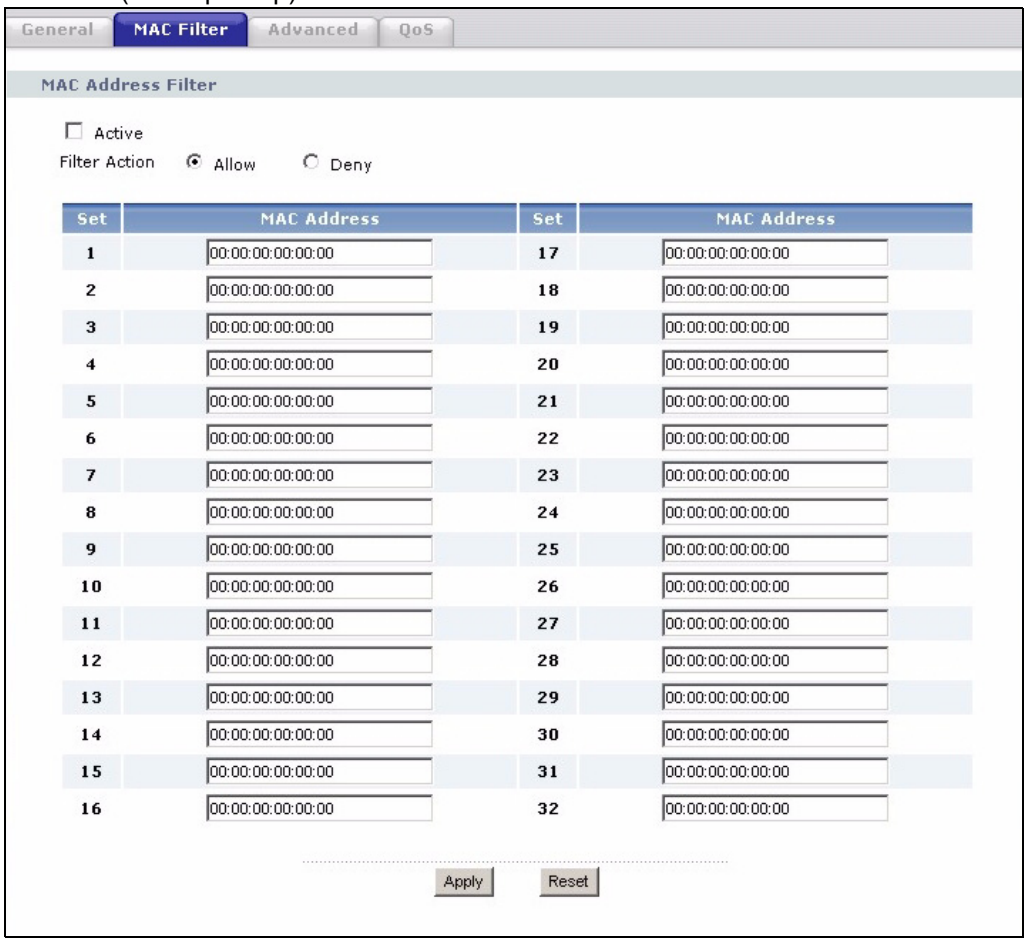
ПОЛЕ	ОПИСАНИЕ
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером учета и NBG334W. Внешний сервер учета и NBG334W должны использовать одинаковый ключ. Этот ключ не передается по сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

4.6 Фильтр MAC-адресов

Окно MAC-фильтра позволяет настроить NBG334W так, чтобы к нему могло получить монопольный доступ до 32 устройств (опция **Allow (Разрешить)**) или, напротив, запретить доступ к NBG334W для данных устройств (опция **Deny (Запретить)**). Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC – Media Access Control – Управление доступом к среде передачи). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02. Для настройки этого окна необходимо знать MAC-адреса устройств.

Для изменения параметров MAC-фильтра NBG334W щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > MAC Filter (MAC-фильтр)**. При этом откроется следующее окно.

Рис. 24 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > MAC Filter (MAC-фильтр)



В следующей таблице даны описания полей этого окна.

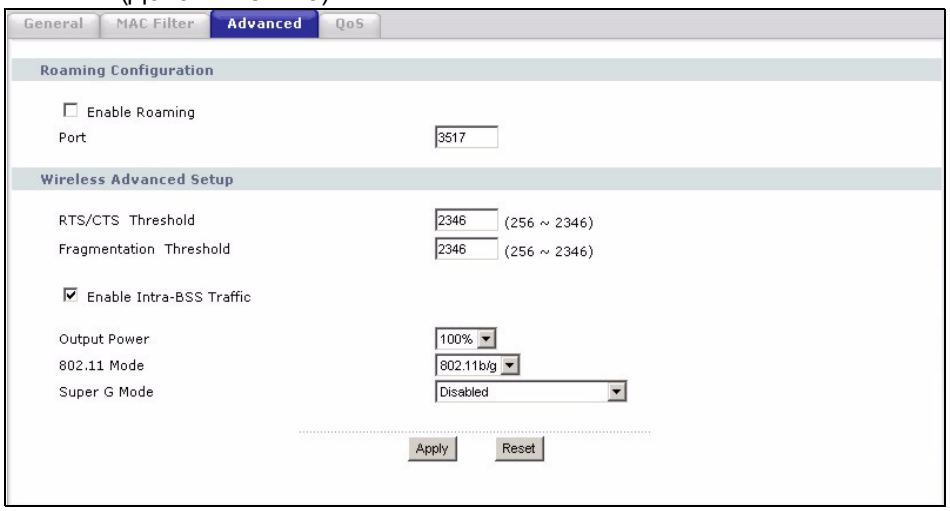
Табл. 15 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > MAC Filter (MAC-фильтр)

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Выберите из раскрывающегося списка **Yes**, чтобы включить фильтрацию MAC-адресов.
Filter Action (Действие фильтра)	Определите способ фильтрации для списка MAC-адресов в таблице **MAC Address**. Выберите **Deny (Запретить)**, чтобы заблокировать доступ к NBG334W. Устройствам с MAC-адресами, не перечисленными в данном списке, доступ к NBG334W будет разрешен. Выберите **Allow (Разрешить)**, чтобы открыть доступ к NBG334W. Устройствам с MAC-адресами, не перечисленными в данном списке, доступ к NBG334W будет запрещен.
Set (Устройство)	Это индексный номер MAC-адреса.
MAC-адрес	Введите в адресные поля MAC-адреса беспроводных станций, которым разрешен или запрещен доступ к NBG334W. MAC-адреса необходимо вводить в специальном формате MAC-адресов, т. е. шесть пар шестнадцатеричных символов, например, 12:34:56:78:9a:bc.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

4.7 Окно расширенных настроек беспроводной локальной сети

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть)** > **Advanced (Дополнительно)**. При этом откроется следующее окно.

Рис. 25 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > Advanced (Дополнительно)



В следующей таблице даны описания полей этого окна.

Табл. 16 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > Advanced (Дополнительно)

ПОЛЕ	ОПИСАНИЕ
Roaming Configuration (Настройка роуминга)	
Enable Roaming (Включить роуминг)	Выберите этот вариант, если в Вашем сетевом окружении находятся несколько точек доступа, между которыми должно переключаться беспроводное устройство.
Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)	
RTS/CTS Threshold (RTS/CTS Порог)	Для данных с размером кадров больше этого значения будет выполняться квитирование RTS (Request To Send – запрос на передачу)/CTS (Clear To Send – готовность к передаче). Если значение RTS/CTS будет больше, чем значение **Fragmentation Threshold (Порог фрагментации)**, то квитирования RTS/CTS не будет, т.к. кадры данных будут фрагментироваться до достижения размера RTS/CTS. Введите значение от 0 до 2432.
Fragmentation Threshold (Порог фрагментации)	Это максимальный размер фрагмента данных, который можно послать. Введите значение от 256 до 2432.
Enable Intra-BSS Traffic (Разрешить трафик Intra-BSS)	BSS (Basic Service Set – Базовый набор служб) используется, если весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети передается через одну точку доступа. Трафик Intra-BSS – это трафик между беспроводными клиентами в пределах одного базового набора служб. При активации Intra-BSS трафика беспроводные клиенты **A** и **B** могут получить доступ к проводной сети и обмениваться информацией между собой. При отключении трафика Intra-BSS беспроводные клиенты **A** и **B** все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией между собой.

Табл. 16 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > Advanced (Дополнительно)

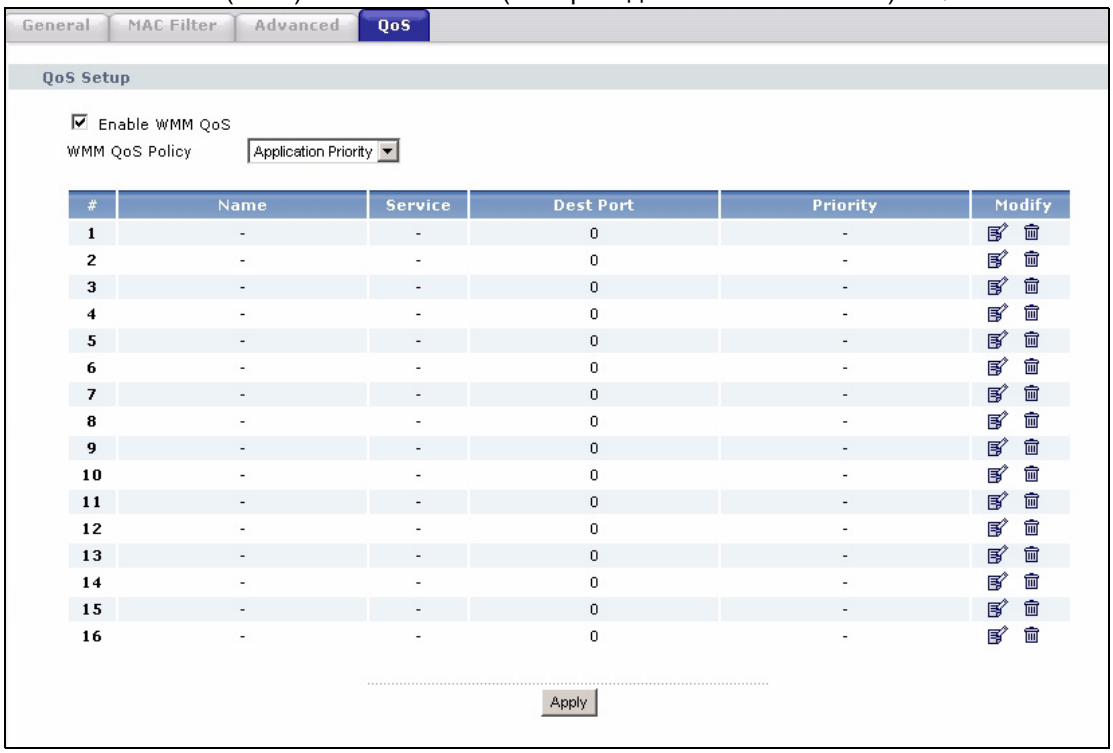
ПОЛЕ	ОПИСАНИЕ
Output Power (Выходная мощность)	В этом поле устанавливается выходная мощность NBG334W. Если в зоне сети высокая плотность точек доступа, следует уменьшить выходную мощность NBG334W, чтобы снизить помехи в других точках доступа.
802.11 Mode (Режим 802.11)	Выберите **«802.11b»**, чтобы разрешить подключение к NBG334W только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11b. Выберите **«802.11g»**, чтобы разрешить подключение к NBG334W только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11g. Выберите **«802.11b/g»**, чтобы разрешить подключение к NBG334W беспроводным устройствам, совместимым как со стандартом IEEE802.11b, так и IEEE802.11g. При этом скорость передачи NBG334W может снизиться.
Super G Mode (Режим Super G)	Это поле включает или выключает функцию Super G. Режим Super G доступен только при выборе варианта **802.11g** или **802.11b/g** в поле **802.11 Mode (Режим 802.11)**. В режиме Super G скорость передачи данных больше, чем в режиме 802.11g. Если Ваши беспроводные клиенты не поддерживают режима Super G, выберите вариант **Disabled (Отключено)**. Выберите вариант **Super G with Dynamic Turbo (Динамический турбо-режим Super G)**, если некоторые или все Ваши беспроводные клиенты поддерживают это режим. В динамическом турбо-режиме для достижения высокой скорости передачи данных используются два объединенных вместе канала. Скорость передачи при этом выше, чем в режиме 802.11g или Super G без динамического турбо-ускорения. Динамическое турбо-ускорение используется только в том случае, когда его поддерживают все устройства сети. При выборе этого режима автоматически выбирается беспроводной канал №6. Выберите вариант **Super G without Turbo (Super G без турбо-ускорения)**, если клиенты в Вашей сети поддерживают Super G, но не поддерживают динамическое турбо-ускорение.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите кнопку **Reset (Сброс)** для восстановления предыдущей конфигурации в этом окне.

4.8 Окно настройки качества обслуживания (QoS)

В окне QoS можно настроить автоматическую раздачу уровней приоритета службам (например, e-mail, VoIP или FTP).

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS**. Появится следующее окно.

Рис. 26 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS



В следующей таблице даны описания полей этого окна.

Табл. 17 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS

ПОЛЕ	ОПИСАНИЕ
Enable WMM QoS (Включить WMM QoS)	Включает функцию WMM QoS (Wireless MultiMedia Quality of Service – качество обслуживания для беспроводной передачи мультимедиа-данных). Интернет-центр NBG334W назначает приоритет пакетам на основе информации о 802.1q или DSCP в их заголовках. Если в заголовке пакета нет информации о WMM, ему назначается стандартный приоритет.
WMM QoS Policy (Политика WMM QoS)	Из раскрывающегося списка выберите **Default (По умолчанию)**, чтобы NBG334W автоматически назначал службе уровень приоритета в соответствии со значением поля «ToS» в IP-заголовке передаваемых пакетов. Функция WMM QoS (Wireless MultiMedia Quality of Service – качество обслуживания для беспроводной передачи мультимедиа-данных) предоставляет приоритет видео- и голосовому трафику, чтобы обеспечить более равномерное его воспроизведение. Выберите **Application Priority (Приоритет приложений)** для перехода к таблице, где отображается информация о названиях приложений, службах, портах и приоритетах для управления с помощью WMM QoS.
	Таблица появляется только в том случае, если выбран вариант **Application Priority (Приоритет приложения)** в поле **WMM QoS Policy (Политика WMM QoS**).
#	Это порядковый номер отдельной записи.
Name (Имя)	В этом поле отображается описание данной записи.
Service (Служба)	В этом поле отображается служба: **FTP**, **WWW**, **E-mail** или **User Defined (Определенная пользователем)**, к которой можно применить WMM QoS.

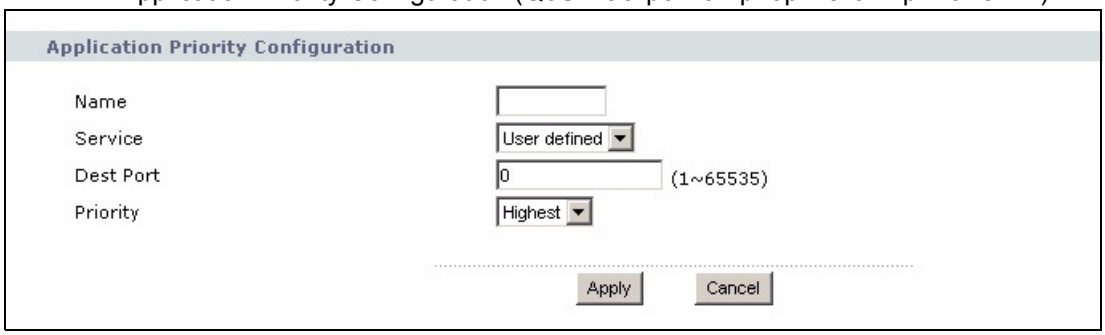
Табл. 17 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS

ПОЛЕ	ОПИСАНИЕ
Dest Port (Порт назначения)	В этом поле отображается номер порта назначения, куда приложение отправляет трафик.
Priority (Приоритет)	В этом поле отображается приоритет приложения. **Highest (Самый высокий)** приоритет используется для высококачественного голосового или видеотрафика. **High (Высокий)** приоритет обычно используется для голосового и видеотрафика среднего качества. **Mid (Средний)** приоритет обычно используется для приложений, не подходящих под вышеуказанные приоритеты. Пример: Интернет-серфинг. **Low (Низкий)** приоритет обычно используется для некритичных «фоновых» приложений, например, для передачи объемных файлов и заданий печати, которые не влияют на работу других приложений.
Modify (Изменить)	Щелкните по значку **Edit (Редактировать)** для отображения окна **Application Priority Configuration (Настройка приоритетов приложений)**. Внесите изменения в существующую запись или создайте новую запись в окне **Application Priority Configuration (Настройка приоритетов приложений)**. Для удаления записи щелкните по значку **Remove (Удалить)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.

4.8.1 Настройка приоритетов приложений

В данном окне можно изменить запись приложения WMM QoS. Для этого щелкните значок редактирования в поле **Modify (Изменить)**. Появится следующее окно.

Рис. 27 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS: Application Priority Configuration (QoS: настройка приоритетов приложений)



См. список широко используемых служб и портов назначения в Прил. F на с. 251.
В следующей таблице даны описания полей этого окна.

Табл. 18 Network (Сеть) > Wireless LAN (Беспроводная локальная сеть) > QoS: Application Priority Configuration (QoS: настройка приоритетов приложений)

ПОЛЕ	ОПИСАНИЕ
Application Priority Configuration (Настройка приоритетов приложений)	
Name (Имя)	Введите описание для приоритета приложения.
Service (Служба)	Здесь представлено описание приложений, которым можно назначать приоритет с помощью WMM QoS. Выберите службу из выпадающего списка. • **E-Mail** Электронная почта позволяет передавать сообщения по компьютерной сети конкретному пользователю или группе пользователей. Существует несколько портов, используемых по умолчанию для электронной почты: POP3 – порт 110 IMAP – порт 143 SMTP – порт 25 HTTP – порт 80 • **FTP** Протокол передачи файлов (FTP) позволяет осуществлять быструю передачу файлов, в том числе файлов большого размера, которые невозможно пересылать с помощью электронной почты. Служба FTP использует порт 21. • **WWW** Всемирная паутина (World Wide Web) – это система в Интернете, предназначенная для распространения графической и текстовой информации, связанной ссылками, на основе протокола передачи гипертекста (Hyper Text Transfer Protocol – HTTP). HTTP – это протокол типа клиент/сервер, разработанный для WWW. Система Web не является синонимом Интернет; точнее, она является одним из сервисов Интернета. Другими сервисами Интернета являются Интернет-чаты (глобальная система, посредством которой пользователи могут общаться друг с другом в реальном времени) и новостные группы (сетевая служба, рассылающая информацию по определенной теме). К службе Web можно подключиться с помощью браузера. • **User-Defined (определяется пользователем)** Определяемые пользователем службы – это специальные службы пользователя, для их настройки требуется установить номер порта и соответствующее приложение.
Dest Port (Порт назначения)	Здесь отображается номер порта, который использует выбранная служба. Введите в поле номер порта, если необходимо использовать порт, отличный от порта по умолчанию.
Priority (Приоритет)	Выберите приоритет из выпадающего списка.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Cancel (Отменить)	Для возврата к предыдущему окну щелкните по кнопке **Cancel (Отменить)**.

5

WAN

В этой главе описывается настройка глобальной сети.

5.1 MAC-адрес порта WAN

В окне настройки MAC-адреса можно настраивать MAC-адрес порта глобальной сети (WAN): использовать заводские настройки или копировать MAC-адрес компьютера в локальной сети. Для использования заводского MAC-адреса выберите вариант **Factory Default (Заводские настройки)**.

В противном случае, щелкните **Clone the computer's MAC address – IP Address (Копировать MAC-адрес компьютера – IP-адрес)** и введите IP-адрес компьютера в локальной сети, чей MAC-адрес предполагается использовать. После успешной настройки адрес будет занесен в файл ПЗУ (конфигурационный файл ZyNOS). Этот адрес не будет меняться до тех пор, пока Вы не измените его самостоятельно или загрузите другой файл ПЗУ. Рекомендуется копировать MAC-адрес до подключения порта WAN.

5.2 Многоадресная рассылка

Как правило, пакеты IP передаются одним из двух способов: одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все абоненты сети). При многоадресной рассылке IP-пакеты пересылаются конкретной группе компьютеров в сети, то есть, не одному компьютеру, но и не всем.

IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки, он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1 см. разделы 4 и 5 RFC 2236. Для идентификации групп узлов используются IP-адреса класса D, которые находятся в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не назначается ни одной группе и используется компьютерами, выполняющими многоадресную рассылку. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все узлы (включая шлюзы). Чтобы участвовать в многоадресной рассылке IGMP, в группу 224.0.0.1 должны входить все узлы. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

NBG334W поддерживает версии IGMP 1 (**IGMP-v1**) и IGMP 2 (**IGMP-v2**). При запуске NBG334W запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации NBG334W периодически обновляет ее. Многоадресную рассылку IP можно включить/отключить для интерфейсов LAN и/или WAN NBG334W с помощью Web-конфигуратора (окна **LAN (Локальная сеть)**, **WAN (Глобальная сеть)**). Для отключения многоадресной рассылки для этих интерфейсов установите **None (Отключить)**.

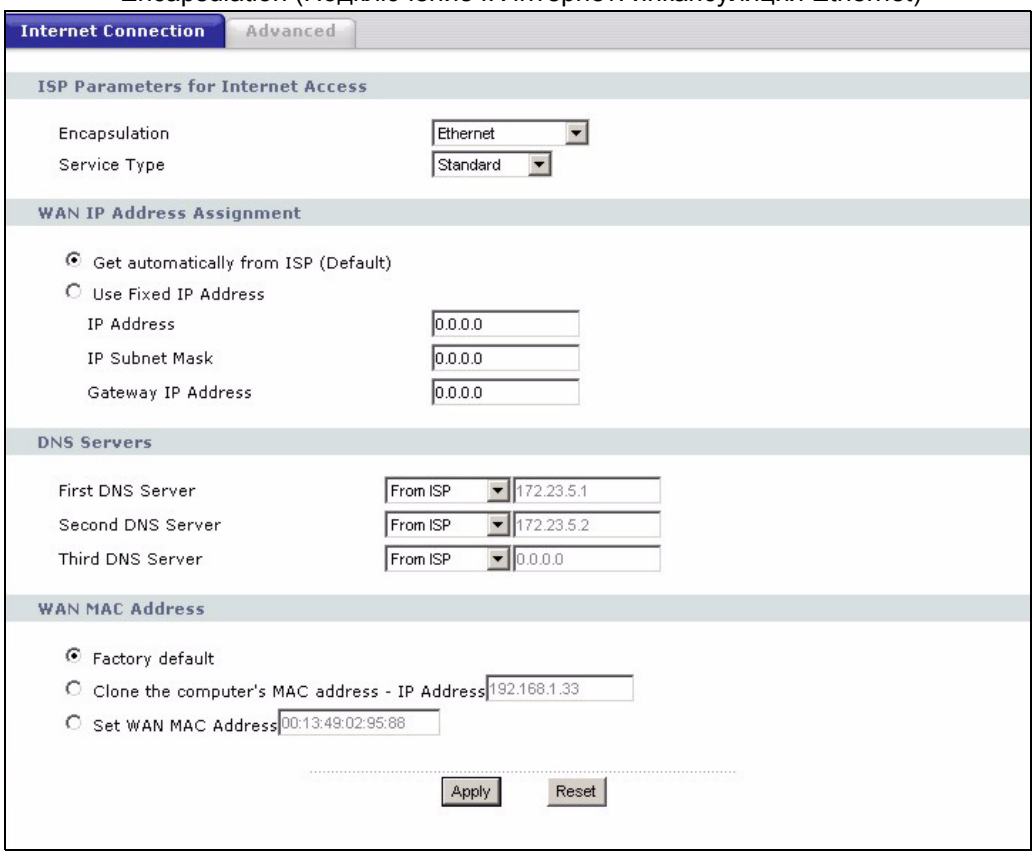
5.3 Подключение к сети Интернет

Это окно используется для изменения параметров доступа интернет-центра NBG334W к сети Интернет. Выберите пункт **Network (Сеть)** > **WAN (Глобальная сеть)**. Вид открывшегося окна будет зависеть от выбранного типа инкапсуляции.

5.3.1 Инкапсуляция Ethernet

Это окно открывается при выборе инкапсуляции **Ethernet**.

Рис. 28 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: Ethernet Encapsulation (Подключение к Интернет: инкапсуляция Ethernet)



В следующей таблице даны описания полей этого окна.

Табл. 19 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: Ethernet Encapsulation (Подключение к Интернет: инкапсуляция Ethernet)

ПОЛЕ	ОПИСАНИЕ
Encapsulation (Инкапсуляция)	Этот вариант следует выбрать в том случае, когда порт WAN используется для обычного Ethernet.
Service Type (Тип обслуживания)	Доступны следующие типы: **Standard (Стандартный)**, **RR-Telstra** (Метод аутентификации RoadRunner Telstra), **RR-Manager** (Метод аутентификации Roadrunner Manager), **RR-Toshiba** (Метод аутентификации Roadrunner Toshiba) и **Telia Login** (Регистрация Telia). Нижеследующие поля не отображаются при выборе типа **«Standard»**.
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Вам поставщиком Интернет-услуг.
Password (Пароль)	Введите пароль для указанного выше имени пользователя.
Retype to Confirm (Повторный ввод для подтверждения)	Повторите ввод пароля для проверки правильности ввода.

Табл. 19 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: Ethernet Encapsulation (Подключение к Интернет: инкапсуляция Ethernet)

ПОЛЕ	ОПИСАНИЕ
Login Server IP Address (IP-адрес сервера регистрации)	Введите в это поле IP-адрес сервера аутентификации, полученный от Вашего поставщика Интернет-услуг. Это поле не отображается при выборе типа **«Telia Login»**.
Login Server (Telia Login only) (Сервер регистрации (Только при выборе типа «Telia Login»))	Введите в это поле доменное имя сервера регистрации Telia, например, «login1.telia.com».
Relogin Every(min) (Telia Login only) (Перерегистрация каждые (мин) (Только при выборе типа «Telia Login»))	Интернет-центр NBG334W должно периодически регистрироваться на сервере Telia. В противном случае, сеанс работы NBG334W на нем будет завершен. Период перерегистрации для NBG334W задается в диапазоне от 1 до 59 минут (по умолчанию, установлено 30).
WAN IP Address Assignment (Назначение IP-адреса в глобальной сети)	
Get automatically from ISP (Автоматически получать от поставщика Интернет-услуг)	Выберите этот вариант, если Ваш поставщик Интернет-услуг не предоставил Вам фиксированного IP-адреса. Этот вариант используется по умолчанию.
Use Fixed IP Address (Использовать фиксированный IP-адрес)	Выберите этот вариант, если поставщик Интернет-услуг предоставил вам фиксированный IP-адрес.
IP Address (IP-адрес)	Если установлен флажок **Use Fixed IP Address (Использовать фиксированный IP-адрес)**, введите в это поле IP-адрес в глобальной сети.
IP Subnet Mask (IP-Маска подсети)	Введите в это поле **IP-маску подсети**.
Gateway IP Address (IP-адрес шлюза)	Введите в это поле **IP-адрес шлюза** (если поставщик Интернет-услуг предоставил его Вам).
DNS Servers (Серверы DNS)	
First DNS Server (Первый сервер DNS) Second DNS Server (Второй сервер DNS) Third DNS Server (Третий сервер DNS)	Выберите вариант **From ISP (Определяется поставщиком Интернет-услуг)**, если Ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN интернет-центра NBG334W). Справа от этого поля отображается (доступный только для чтения) IP-адрес сервера DNS, назначенный поставщиком интернет-услуг. Если Вам известен IP-адрес сервера DNS, выберите вариант **User-Defined (Определяется пользователем)**. Введите этот адрес в поле справа от данного поля. Если выбрать вариант **User-Defined (Определяется пользователем)**, но не указать IP-адрес, то при нажатии на кнопку **Apply (Применить)** вариант **User-Defined** сменится на **None (Отключить)**. Если для второго сервера выбрать вариант **User-Defined (Определяется пользователем)** и указать точно такой же адрес, то при нажатии на кнопку **Apply (Применить)** он поменяется на **None (Нет)**. Если Вы не хотите настраивать серверы DNS, выберите вариант **«None»**. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.

Табл. 19 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: Ethernet Encapsulation (Подключение к Интернет: инкапсуляция Ethernet)

ПОЛЕ	ОПИСАНИЕ
WAN MAC Address (MAC-адрес порта WAN)	В разделе настройки MAC-адреса нужно указать MAC-адрес порта WAN интернет-центра NBG334W путем копирования MAC-адреса компьютера локальной сети или путем ручного ввода.
Factory default (Заводские настройки)	Для использования заводского MAC-адреса выберите вариант **Factory default (Заводские настройки)**.
Clone the computer's MAC address (Копировать MAC-адрес компьютера)	Выберите вариант **Clone the computer's MAC address (Копировать MAC-адрес компьютера)** и введите IP-адрес компьютера в локальной сети, чей MAC-адрес предполагается использовать. После успешной настройки адрес будет занесен в файл ПЗУ (конфигурационный файл ZyNOS). Этот адрес не будет меняться до тех пор, пока Вы не измените его самостоятельно или не загрузите другой файл ПЗУ.
Set WAN MAC Address (Введите MAC-адрес порта WAN)	Введите сюда MAC-адрес, который хотите использовать.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

5.3.2 Инкапсуляция PPPoE

Интернет-центр NBG334W поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet – Протокол «точка-точка» поверх Ethernet). PPPoE – это стандарт IETF (RFC 2516), определяющий, каким образом персональный компьютер (PC) взаимодействует с выделенной линией Ethernet (DSL, кабель, беспроводной канал и т.д.). Для коммутируемого подключения через PPPoE следует выбрать пункт **PPP over Ethernet**.

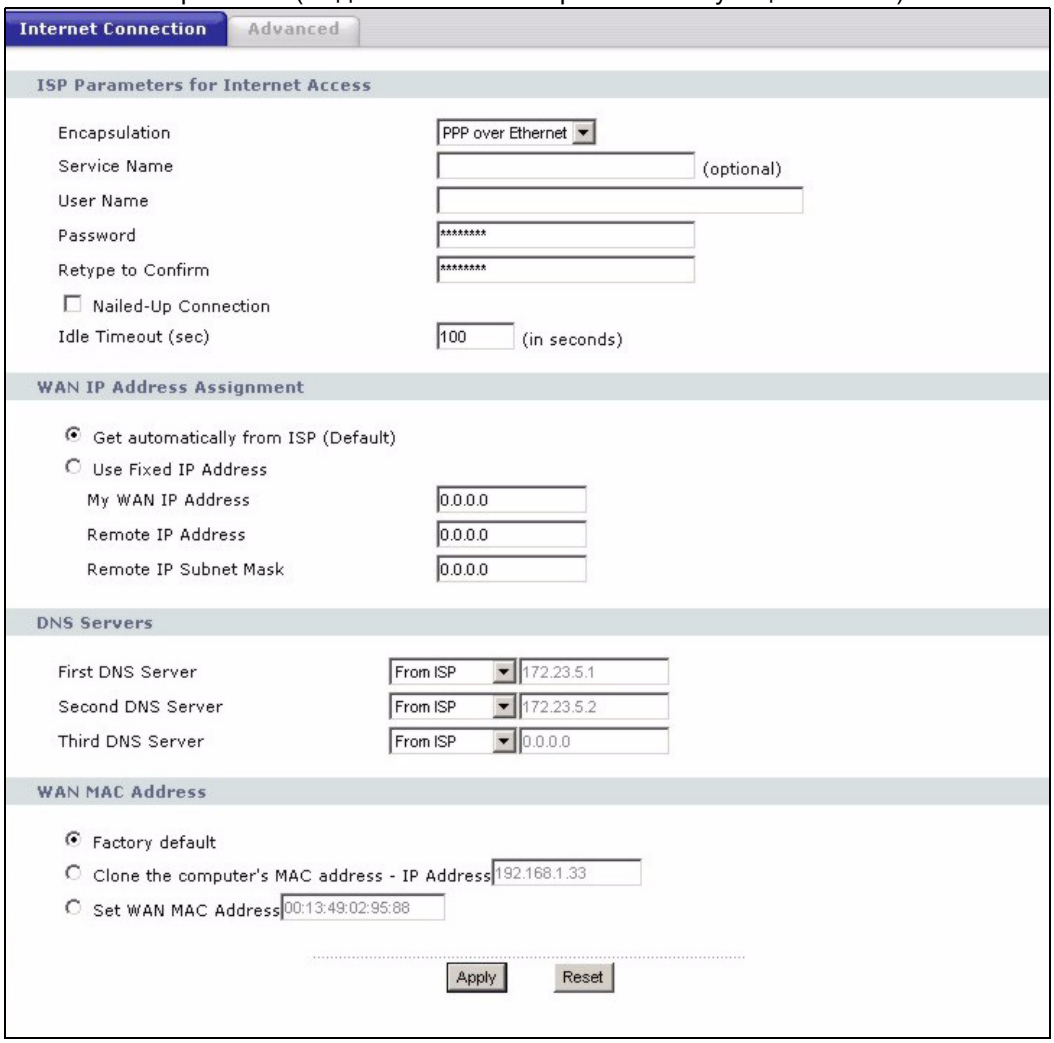
Для провайдера услуг протокол PPPoE обеспечивает метод доступа и аутентификации, который работает с существующими системами управления доступом (например, RADIUS).

Одним из преимуществ PPPoE является возможность доступа пользователей к нескольким сетевым службам, т. е. функция, называемая динамическим выбором служб. Это позволяет провайдеру услуг легко создавать и предоставлять конкретным пользователям новые услуги IP.

Так как PPPoE выполняется непосредственно на NBG334W (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта процедура полностью выполняется интернет-центром NBG334W. Кроме того, при включении функции NAT доступ будут иметь все компьютеры локальной сети.

Это окно открывается при выборе инкапсуляции **PPPoE**.

Рис. 29 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPPoE Encapsulation (Подключение к Интернет: инкапсуляция PPPoE)



В следующей таблице даны описания полей этого окна.

Табл. 20 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPPoE Encapsulation (Подключение к Интернет: инкапсуляция PPPoE)

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access (Параметры доступа в Интернет от поставщика Интернет-услуг)	
Encapsulation (Инкапсуляция)	Для коммутируемого подключения через PPPoE следует выбрать пункт **PPP over Ethernet**. Интернет-центр NBG334W поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet – Протокол «точка-точка» поверх Ethernet). PPPoE – это проект стандарта IETF (RFC 2516), который определяет порядок взаимодействия персонального компьютера (PC) с выделенной линией Ethernet (xDSL, кабельным, беспроводным и т.д.) соединением. В случае установки PPPoE прямо на маршрутизаторе, а не на отдельных компьютерах, установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта часть задачи выполняется маршрутизатором. Кроме того, при включении функции NAT доступ будут иметь все компьютеры локальной сети.

Табл. 20 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPPoE Encapsulation (Подключение к Интернет: инкапсуляция PPPoE)

ПОЛЕ	ОПИСАНИЕ
Service Name (Название службы)	Выберите предоставленное Вам название службы PPPoE. Это название используется службой PPPoE для обнаружения сервера PPPoE.
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Вам поставщиком Интернет-услуг.
Password (Пароль)	Введите пароль для указанного выше имени пользователя.
Retype to Confirm (Повторный ввод для подтверждения)	Повторите ввод пароля для проверки правильности ввода.
Nailed-Up Connection (Постоянное подключение)	Выберите этот вариант, если хотите, чтобы подключение было постоянным.
Idle Timeout (Время простоя)	В этом поле вводится время (в секундах), по истечении которого маршрутизатор должен автоматически отключаться от сервера PPPoE.
WAN IP Address Assignment (Назначение IP-адреса в глобальной сети)	
Get automatically from ISP (Автоматически получать от поставщика Интернет-услуг)	Выберите этот вариант, если Ваш поставщик Интернет-услуг не предоставил Вам фиксированного IP-адреса. Этот вариант используется по умолчанию.
Use Fixed IP Address (Использовать фиксированный IP-адрес)	Выберите этот вариант, если поставщик Интернет-услуг предоставил вам фиксированный IP-адрес.
My WAN IP Address (Мой IP-адрес в глобальной сети)	Если установлен флажок **Use Fixed IP Address (Использовать фиксированный IP-адрес)**, введите в это поле IP-адрес в глобальной сети.
Remote IP address (Удаленный IP-адрес)	Введите в это поле удаленный IP-адрес (если поставщик Интернет-услуг предоставил его Вам).
Remote IP Subnet Mask (Маска IP подсети удаленного узла)	Введите в это поле маску подсети удаленного IP-адреса.

Табл. 20 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPPoE Encapsulation (Подключение к Интернет: инкапсуляция PPPoE)

ПОЛЕ	ОПИСАНИЕ
DNS Servers (Серверы DNS)	
First DNS Server (Первый сервер DNS) Second DNS Server (Второй сервер DNS) Third DNS Server (Третий сервер DNS)	Выберите вариант **From ISP (Определяется поставщиком Интернет-услуг)**, если Ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN интернет-центра NBG334W). Справа от этого поля отображается (доступный только для чтения) IP-адрес сервера DNS, назначенный поставщиком интернет-услуг. Если Вам известен IP-адрес сервера DNS, выберите вариант **User-Defined (Определяется пользователем)**. Введите этот адрес в поле справа от данного поля. Если выбрать вариант **User-Defined (Определяется пользователем)**, но не указать IP-адрес, то при нажатии на кнопку **Apply (Применить)** вариант **User-Defined (Определяется пользователем)** сменится на **None (Отключить)**. Если для второго сервера выбрать вариант **User-Defined (Определяется пользователем)** и указать точно такой же адрес, то при нажатии на кнопку **Apply (Применить)** он поменяется на **None (Нет)**. Если Вы не хотите настраивать серверы DNS, выберите вариант **«None»**. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.
WAN MAC Address (MAC-адрес порта WAN)	В разделе настройки MAC-адреса нужно указать MAC-адрес порта WAN интернет-центра NBG334W путем копирования MAC-адреса компьютера локальной сети или путем ручного ввода.
Factory default (Заводские настройки)	Для использования заводского MAC-адреса выберите вариант **Factory default (Заводские настройки)**.
Clone the computer's MAC address (Копировать MAC-адрес компьютера)	Выберите вариант **Clone the computer's MAC address (Копировать MAC-адрес компьютера)** и введите IP-адрес компьютера в локальной сети, чей MAC-адрес предполагается использовать. После успешной настройки адрес будет занесен в файл ПЗУ (конфигурационный файл ZyNOS). Этот адрес не будет меняться до тех пор, пока Вы не измените его самостоятельно или не загрузите другой файл ПЗУ.
Set WAN MAC Address (Введите MAC-адрес порта WAN)	Введите сюда MAC-адрес, который хотите использовать.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

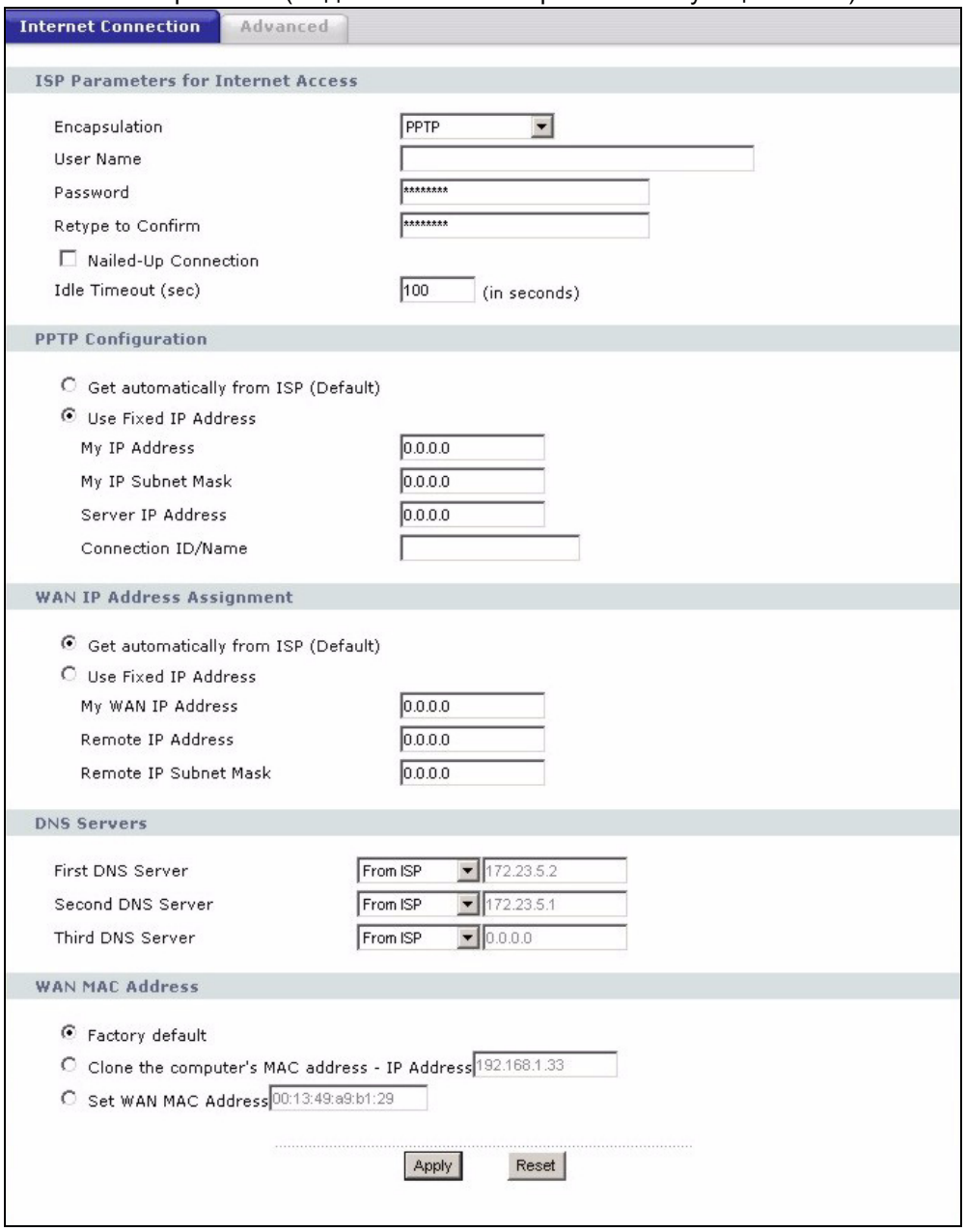
5.3.3 Инкапсуляция PPTP

Сетевой протокол туннелирования «точка-точка» (PPTP: Point-to-Point Tunneling Protocol) обеспечивает защищенную передачу данных от удаленного клиента до частного сервера, создавая для этого виртуальную частную сеть (VPN: Virtual Private Network) в сетях, основанных на протоколе TCP/IP.

Протокол PPTP, по запросу, поддерживает создание мультипротокольных и виртуальных частных сетей в таких общедоступных сетях, как Интернет.

Это окно открывается при выборе инкапсуляции **PPTP**.

Рис. 30 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPTP Encapsulation (Подключение к Интернет: инкапсуляция PPTP)



В следующей таблице даны описания полей этого окна.

Табл. 21 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPTP Encapsulation (Подключение к Интернет: инкапсуляция PPTP)

ПОЛЕ	ОПИСАНИЕ
ISP Parameters for Internet Access (Параметры доступа в Интернет от поставщика Интернет-услуг)	
Encapsulation (Инкапсуляция)	Сетевой протокол туннелирования «точка-точка» (PPTP: Point-to-Point Tunneling Protocol) обеспечивает защищенную передачу данных от удаленного клиента до частного сервера, создавая для этого виртуальную частную сеть (VPN: Virtual Private Network) в сетях, основанных на протоколе TCP/IP. Протокол PPTP, по запросу, поддерживает создание мультипротокольных и виртуальных частных сетей в таких общедоступных сетях, как Интернет. Интернет-центр NBG334W одновременно поддерживает подключение только к одному серверу PPTP. Для настройки клиента PPTP следует заполнить поля **User Name (Имя пользователя)** и **Password (Пароль)** для PPP-подключения и параметры PPTP для PPTP-подключения.
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Вам поставщиком Интернет-услуг.
Password (Пароль)	Введите пароль для указанного выше имени пользователя.
Retype to Confirm (Повторный ввод для подтверждения)	Повторите ввод пароля для проверки правильности ввода.
Nailed-Up Connection (Постоянное подключение)	Выберите этот вариант, если хотите, чтобы подключение было постоянным.
Idle Timeout (Время простоя)	В этом поле вводится время (в секундах), по истечении которого маршрутизатор NBG334W должен автоматически отключаться от сервера PPTP.
PPTP Configuration (Настройка PPTP)	
Get automatically from ISP (Автоматически получать от поставщика Интернет-услуг)	Выберите этот вариант, если Ваш поставщик Интернет-услуг не предоставил Вам фиксированного IP-адреса. Этот вариант используется по умолчанию.
Use Fixed IP Address (Использовать фиксированный IP-адрес)	Выберите этот вариант, если поставщик Интернет-услуг предоставил вам фиксированный IP-адрес.
My IP Address (Собственный IP-адрес)	Введите в это поле (статический) IP-адрес, предоставленный Вам поставщиком Интернет-услуг.
My IP Subnet Mask (Маска подсети собственного IP-адреса)	NBG334W вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную NBG334W.
Server IP Address (IP-адрес сервера)	Введите IP-адрес PPTP сервера.

Табл. 21 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPTP Encapsulation (Подключение к Интернет: инкапсуляция PPTP)

ПОЛЕ	ОПИСАНИЕ
Connection ID/ Name (Идентификатор/ имя подключения)	Введите в это поле имя, идентифицирующее сервер PPTP.
WAN IP Address Assignment (Назначение IP-адреса в глобальной сети)	
Get automatically from ISP (Автоматически получать от поставщика Интернет-услуг)	Выберите этот вариант, если Ваш поставщик Интернет-услуг не предоставил Вам фиксированного IP-адреса. Этот вариант используется по умолчанию.
Use Fixed IP Address (Использовать фиксированный IP-адрес)	Выберите этот вариант, если поставщик Интернет-услуг предоставил вам фиксированный IP-адрес.
My WAN IP Address (Собственный IP-адрес в глобальной сети)	Если установлен флажок **Use Fixed IP Address (Использовать фиксированный IP-адрес)**, введите в это поле IP-адрес в глобальной сети.
Remote IP address (Удаленный IP-адрес)	Введите в это поле удаленный IP-адрес (если поставщик Интернет-услуг предоставил его Вам).
Remote IP Subnet Mask (Маска подсети удаленного узла)	Введите в это поле маску подсети удаленного IP-адреса.
DNS Servers (Серверы DNS)	
First DNS Server (Первый сервер DNS) Second DNS Server (Второй сервер DNS) Third DNS Server (Третий сервер DNS)	Выберите вариант **From ISP (Определяется поставщиком Интернет-услуг)**, если Ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN интернет-центра NBG334W). Справа от этого поля отображается (доступный только для чтения) IP-адрес сервера DNS, назначенный поставщиком интернет-услуг. Если Вам известен IP-адрес сервера DNS, выберите вариант **User-Defined (Определяется пользователем)**. Введите этот адрес в поле справа от данного поля. Если выбрать вариант **User-Defined (Определяется пользователем)**, но не указать IP-адрес, то при нажатии на кнопку **Apply (Применить)** вариант **User-Defined (Определяется пользователем)** сменится на **None (Отключить)**. Если для второго сервера выбрать вариант **User-Defined (Определяется пользователем)** и указать точно такой же адрес, то при нажатии на кнопку **Apply (Применить)** он поменяется на **None (Нет)**. Если Вы не хотите настраивать серверы DNS, выберите вариант **«None»**. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.
WAN MAC Address (MAC-адрес порта WAN)	В разделе настройки MAC-адреса нужно указать MAC-адрес порта WAN интернет-центра NBG334W путем копирования MAC-адреса компьютера локальной сети или путем ручного ввода.
Factory default (Заводские настройки)	Для использования заводского MAC-адреса выберите вариант **Factory default (Заводские настройки)**.

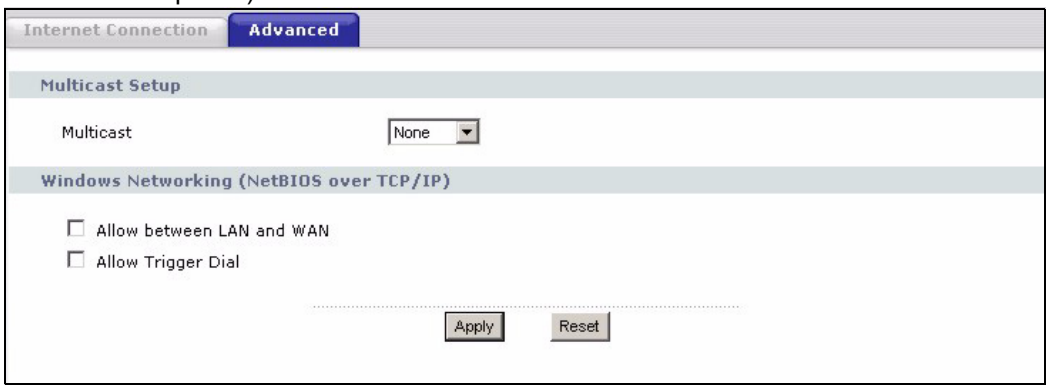
Табл. 21 Network (Сеть) > WAN (Глобальная сеть) > Internet Connection: PPTP Encapsulation (Подключение к Интернет: инкапсуляция PPTP)

ПОЛЕ	ОПИСАНИЕ
Clone the computer's MAC address (Копировать MAC-адрес компьютера)	Выберите вариант **Clone the computer's MAC address (Копировать MAC-адрес компьютера)** и введите IP-адрес компьютера в локальной сети, чей MAC-адрес предполагается использовать. После успешной настройки адрес будет занесен в файл ПЗУ (конфигурационный файл ZyNOS). Этот адрес не будет меняться до тех пор, пока Вы не измените его самостоятельно или не загрузите другой файл ПЗУ.
Set WAN MAC Address (Введите MAC-адрес порта WAN)	Введите сюда MAC-адрес, который хотите использовать.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

5.4 Окно расширенной настройки глобальной сети

Для редактирования дополнительных параметров подключения интернет-центра NBG334W к глобальной сети выберите пункт **Network (Сеть)** > **WAN (Глобальная сеть)** > **Advanced (Дополнительные настройки)**. При этом откроется следующее окно.

Рис. 31 Network (Сеть) > WAN (Глобальная сеть) > Advanced (Дополнительные настройки)



В следующей таблице даны описания полей этого окна.

Табл. 22 WAN (Глобальная сеть) > Advanced (Дополнительные настройки)

ПОЛЕ	ОПИСАНИЕ
Multicast Setup (Настройка многоадресной рассылки)	
Multicast (Многоадресная рассылка)	Выберите один из следующих вариантов: **IGMP V-1**, **IGMP V-2** или **None (Нет)**. IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки, он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1 см. разделы 4 и 5 RFC 2236.
Организация сети в Windows (NetBIOS через TCP/IP): NetBIOS (Network Basic Input/Output System – Сетевая базовая система ввода-вывода) – это многоадресная рассылка TCP- или UDP-пакетов, позволяющая компьютеру подключаться и обмениваться информацией с локальной сетью. Для некоторых служб с автоматическим набором номера, например PPPoE или PPTP, пакеты NetBIOS могут инициировать нежелательные вызовы. Несмотря на это, иногда необходимо разрешить прохождение пакетов NetBIOS в глобальную сеть для того, чтобы найти компьютер в глобальной сети.	
Allow between LAN and WAN (Разрешить передачу между LAN и WAN)	Поставьте в этом поле флажок, чтобы разрешить передачу пакетов NetBIOS из локальной сети в глобальную сеть и наоборот. Если в межсетевом экране установлена политика по умолчанию, которая блокирует трафик из глобальной сети в локальную сеть, необходимо включить правило межсетевого экрана, которое пропускает трафик NetBIOS из глобальной сети в локальную. Снимите флажок в этом поле, чтобы блокировать передачу всех пакетов NetBIOS из локальной сети в глобальную сеть и наоборот.
Allow Trigger Dial (Разрешить инициацию вызовов)	Эта опция разрешает пакетам NetBIOS инициировать вызовы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

6

LAN

В этой главе описывается настройка параметров локальной сети.

6.1 Общая информация о локальной сети

LAN (Local Area Network – Локальная сеть) – это коллективно используемая система связи, к которой подключено множество компьютеров. Локальная сеть представляет собой компьютерную сеть, ограниченную ближайшей территорией, обычно это здание или этаж в здании. Окна настройки локальной сети позволяют настроить сервер DHCP, управлять IP-адресами, а также разделить физическую сеть на логические подсети.

6.1.1 Настройка диапазона IP-адресов

По умолчанию интернет-центр NBG334W настроен на использование диапазона из 32 IP-адресов, начиная от 192.168.1.33 и заканчивая 192.168.1.64. Такая конфигурация допускает возможность использования 31 IP-адреса (за вычетом самого NBG334W) в нижнем диапазоне (от 192.168.1.2 до 192.168.1.32) для других серверов, например, почтовых, FTP-, TFTP-, веб-серверов и т.д.

6.2 Настройка TCP/IP локальной сети

Интернет-центр NBG334W обладает функцией встроенного сервера DHCP, которая позволяет назначать IP-адреса и серверы DNS компьютерам с установленным клиентом DHCP.

6.2.1 Стандартные заводские настройки локальной сети

Интернет-центр NBG334W имеет следующие заводские настройки локальной сети:

- IP-адрес: 192.168.1.1, маска подсети: 255.255.255.0 (24 бита)
- Сервер DHCP: включен, используются 32 клиентских IP-адреса, начиная с 192.168.1.33.

Эти параметры должны работать в большинстве случаев. Если поставщик Интернет-услуг предоставил явный адрес(а) сервера DNS, то информацию о том, какие поля подлежат настройке, см. в справке по расширенному веб-конфигуратору.

6.2.2 Многоадресная рассылка

Как правило, пакеты IP передаются одним из двух способов: одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все абоненты сети). При многоадресной рассылке IP-пакеты пересылаются конкретной группе компьютеров в сети, то есть, не одному компьютеру, но и не всем.

IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки, он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1 см. разделы 4 и 5 RFC 2236. Для идентификации групп узлов используются IP-адреса класса D, которые находятся в диапазоне от 224.0.0.0 до 239.255.255.255. Адрес 224.0.0.0 не назначается ни одной группе и используется компьютерами, осуществляющими многоадресную рассылку IP. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все узлы (включая шлюзы). Для участия в IGMP узел должен принадлежать к группе 224.0.0.1. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

NBG334W поддерживает версии IGMP 1 (**IGMP-v1**) и IGMP 2 (**IGMP-v2**). При запуске NBG334W запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации NBG334W периодически обновляет ее. Многоадресную рассылку IP можно включить/отключить для интерфейсов LAN и/или WAN NBG334W с помощью Web-конфигуратора (окна **LAN (Локальная сеть)**, **WAN (Глобальная сеть)**). Для отключения многоадресной рассылки для этих интерфейсов выберите **None (Нет)**.

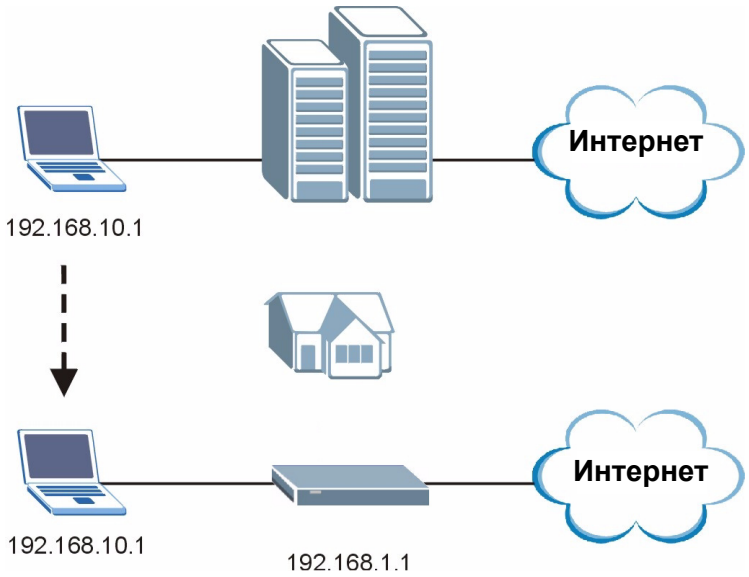
6.2.3 Функция Any IP (Любой IP)

Чтобы предоставить компьютеру доступ в Интернет через NBG334W, необходимо, чтобы IP-адреса и маски подсети компьютера и NBG334W находились в одной и той же подсети. В случае, если компьютеру необходимо использовать статический IP-адрес, принадлежащий другой сети, вам придется устанавливать сетевые настройки компьютера вручную каждый раз, когда нужно получить доступ в Интернет через NBG334W.

Если в NBG334W включены функции Any IP и NAT, компьютер может получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и NBG334W находятся в разных подсетях. Независимо от того, динамический или статический IP-адрес назначен компьютеру, вы можете просто подключить компьютер к NBG334W для получения доступа в Интернет.

На следующем рисунке изображен сценарий, где компьютер использует статический частный IP-адрес в корпоративной среде. При установке NBG334W в жилом доме можно получить доступ в Интернет без изменения сетевых настроек компьютера, даже если IP-адреса компьютера и NBG334W находятся в разных подсетях.

Рис. 32 Пример Any IP (Любого IP)



Функция Any IP не применяется к компьютерам с динамическим или статическим IP-адресом, принадлежащим к той же подсети, что и IP-адрес NBG334W.

Для использования в NBG334W функции Any IP *необходимо* включить трансляцию сетевых адресов (NAT).

ARP (Address Resolution Protocol – Протокол разрешения адресов) служит для установления соответствия между адресом межсетевого протокола IP (IP-адрес) и аппаратным адресом компьютера в локальной сети, известного также как Media Access Control (Управление доступом к среде) или MAC-адрес. Таблица маршрутизации IP устройства Ethernet (NBG334W) определяет следующий транзитный пункт, который необходимо использовать для пересылки данных конкретному адресату.

Когда компьютер пытается в первый раз получить доступ в Интернет через NBG334W, выполняются следующие действия.

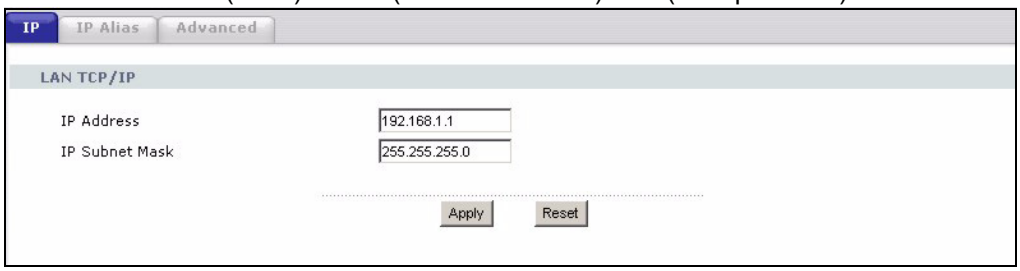
1. Если компьютер (находящийся в другой подсети) пытается в первый раз получить доступ в Интернет, он посылает пакеты на шлюз по умолчанию (не NBG334W) с помощью поиска его MAC-адреса в своей таблице ARP.
2. Если компьютер не может обнаружить шлюз по умолчанию, посылается широковещательный запрос ARP по локальной сети.
3. NBG334W принимает запрос ARP и отвечает компьютеру, посылая ему свой MAC-адрес.
4. Компьютер обновляет MAC-адрес шлюза по умолчанию в таблице ARP. Обновив таблицу ARP, компьютер может подключаться к Интернет через NBG334W.
5. При получении пакетов от компьютера NBG334W создает запись в таблице маршрутизации IP, с тем чтобы правильно пересылать пакеты, предназначенные для этого компьютера.

После обновления информации о маршрутизации компьютер получает доступ к NBG334W и к сети Интернет, как будто он находится в той же подсети, что и NBG334W.

6.3 Окно настройки локальной IP-сети

Это окно используется для изменения основных настроек локальной сети. Выберите пункт **Network (Сеть)** > **LAN (Локальная сеть)**.

Рис. 33 Network (Сеть) > LAN (Локальная сеть) > IP (Настройки IP)



В следующей таблице даны описания полей этого окна.

Табл. 23 Network (Сеть) > LAN (Локальная сеть) > IP (Настройки IP)

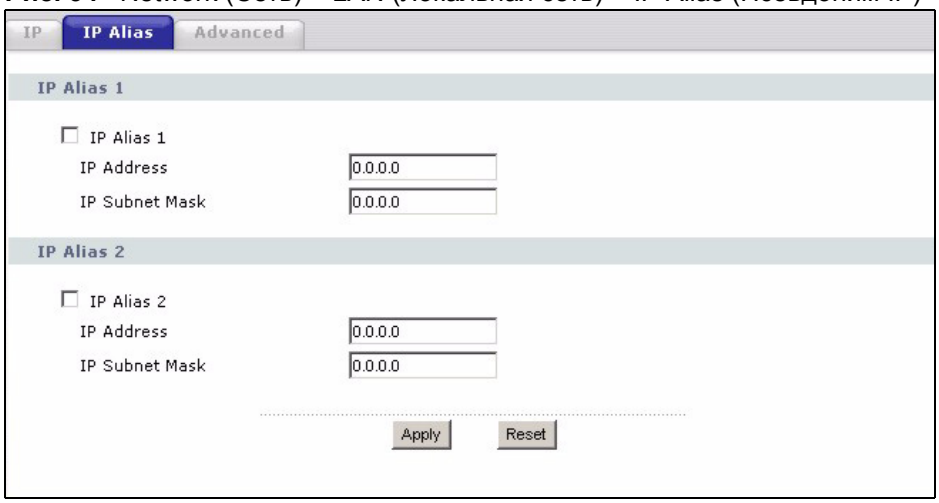
ПОЛЕ	ОПИСАНИЕ
LAN TCP/IP (Настройка TCP/IP локальной сети)	
IP Address (IP-адрес)	Введите в это поле IP-адрес интернет-центра NBG334W в десятичном представлении с точками 192.168.1.1 (используется по умолчанию).
IP Subnet Mask (IP-Маска подсети)	Маска подсети определяет сетевую часть IP-адреса. NBG334W вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную NBG334W.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

6.4 Псевдоним IP локальной сети

Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей на основе одного интерфейса Ethernet. NBG334W поддерживает три логических интерфейса локальной сети через один физический интерфейс Ethernet, причем NBG334W является шлюзом для каждой локальной сети.

Для изменения в NBG334W настроек псевдонимов IP щелкните **Network (Сеть) > LAN (Локальная сеть) > IP Alias (Псевдоним IP)**. При этом откроется следующее окно.

Рис. 34 Network (Сеть) > LAN (Локальная сеть) > IP Alias (Псевдоним IP)



В следующей таблице даны описания полей этого окна.

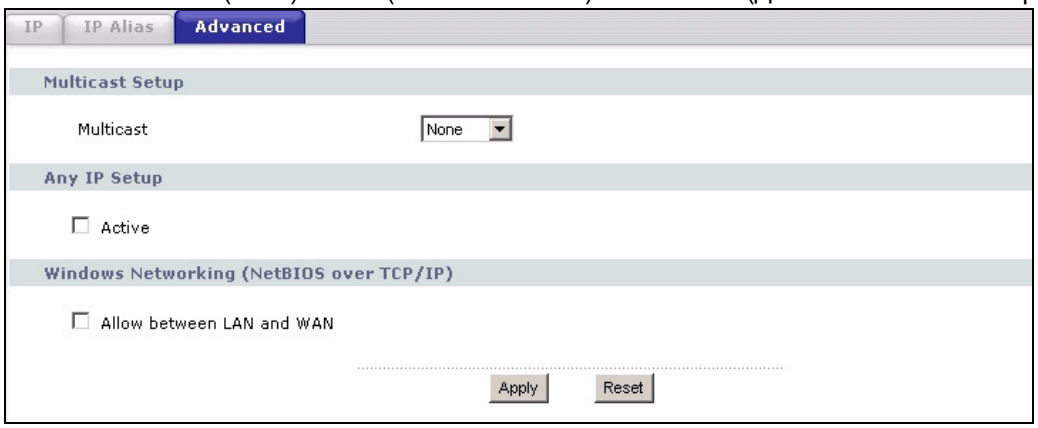
Табл. 24 Network (Сеть) > LAN (Локальная сеть) > IP Alias (Псевдоним IP)

ПОЛЕ	ОПИСАНИЕ
IP Alias 1,2 (Псевдоним IP 1, 2)	Поставьте флажок для настройки другой локальной сети в NBG334W.
IP Address (IP-адрес)	Введите IP-адрес NBG334W в десятичном виде с разделительными точками.
IP Subnet Mask (IP-Маска подсети)	NBG334W вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную NBG334W.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

6.5 Окно расширенной настройки локальной сети

Для редактирования дополнительных параметров IP-подключения интернет-центра NBG334W к локальной сети выберите пункт **Network (Сеть)** > **LAN (Локальная сеть)** > **Advanced (Дополнительные настройки)**. При этом откроется следующее окно.

Рис. 35 Network (Сеть) > LAN (Локальная сеть) > Advanced (Дополнительные настройки)



В следующей таблице даны описания полей этого окна.

Табл. 25 Network (Сеть) > LAN (Локальная сеть) > Advanced (Дополнительные настройки)

ПОЛЕ	ОПИСАНИЕ
Multicast (Многоадресная рассылка)	Выберите один из следующих вариантов: **IGMP V-1**, **IGMP V-2** или **None (Нет)**. IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки, он не предназначен для передачи пользовательских данных. Версия 2 IGMP (RFC 2236) является усовершенствованным вариантом версии 1 (RFC 1112), однако версия 1 IGMP по-прежнему широко используется. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1, см. разделы 4 и 5 RFC 2236.
Any IP Setup (Настройка Any IP)	
Active (Активировать)	Эта опция позволяет компьютерам из разных подсетей использовать интернет-центр NBG334W.
Организация сети в Windows (NetBIOS через TCP/IP): NetBIOS (Network Basic Input/Output System – Сетевая базовая система ввода-вывода) – это многоадресная рассылка TCP- или UDP-пакетов, позволяющая компьютеру подключаться и обмениваться информацией с локальной сетью. Для некоторых служб с автоматическим набором номера, например PPPoE или PPTP, пакеты NetBIOS инициируют нежелательные вызовы. Несмотря на это, иногда необходимо разрешить прохождение пакетов NetBIOS в глобальную сеть для того, чтобы найти компьютер в глобальной сети.	
Allow between LAN and WAN (Разрешить передачу между LAN и WAN)	Поставьте в этом поле флажок, чтобы разрешить передачу пакетов NetBIOS из локальной сети в глобальную сеть и наоборот. Если в межсетевом экране установлена политика по умолчанию, которая блокирует трафик из глобальной сети в локальную сеть, необходимо включить правило межсетевого экрана, которое пропускает трафик NetBIOS из глобальной сети в локальную. Снимите флажок в этом поле, чтобы блокировать передачу всех пакетов NetBIOS из локальной сети в глобальную сеть и наоборот.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

7

DHCP

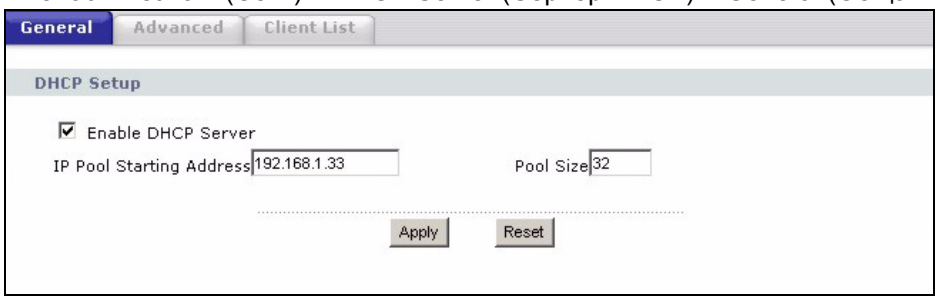
7.1 DHCP

DHCP (Dynamic Host Configuration Protocol – Протокол динамической настройки узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать настройки TCP/IP при загрузке от центрального сервера DHCP. Можно настроить NBG334W как сервер DHCP или отключить эту функцию. При работе в режиме сервера NBG334W предоставляет клиентами DHCP конфигурацию TCP/IP. Если служба DHCP отключена, то для нормальной работы в локальной сети необходим другой сервер DHCP, в противном случае придется настраивать компьютер вручную.

7.2 Окно общей настройки сервера DHCP

Выберите пункт **Network (Сеть)** > **DHCP Server (Сервер DHCP)**. Появится следующее окно.

Рис. 36 Network (Сеть) > DHCP Server (Сервер DHCP) > General (Общая настройка)



В следующей таблице даны описания полей этого окна.

Табл. 26 Network (Сеть) > DHCP Server (Сервер DHCP) > General (Общая настройка)

ПОЛЕ	ОПИСАНИЕ
Enable DHCP Server (Включить сервер DHCP)	DHCP (Dynamic Host Configuration Protocol – Протокол динамической настройки узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентам (компьютерам) при загрузке получать настройки TCP/IP от центрального сервера DHCP. Если Ваш поставщик Интернет-услуг не предоставил Вам другие инструкции, оставьте флажок в поле **Enable DHCP Server (Включить сервер DHCP)**. Чтобы отключить функцию сервера DHCP на интернет-центре NBG334W, снимите этот флажок. При работе в режиме сервера NBG334W предоставляет клиентами DHCP конфигурацию TCP/IP. Если служба DHCP отключена, то для нормальной работы в локальной сети необходим другой сервер DHCP, в противном случае придется настраивать компьютеры вручную. Если используется режим сервера, следует заполнить следующие четыре поля.
IP Pool Starting Address (Первый адрес пула IP-адресов)	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.
Pool Size (Размер пула)	В этом поле задается размер пула непрерывных IP-адресов.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

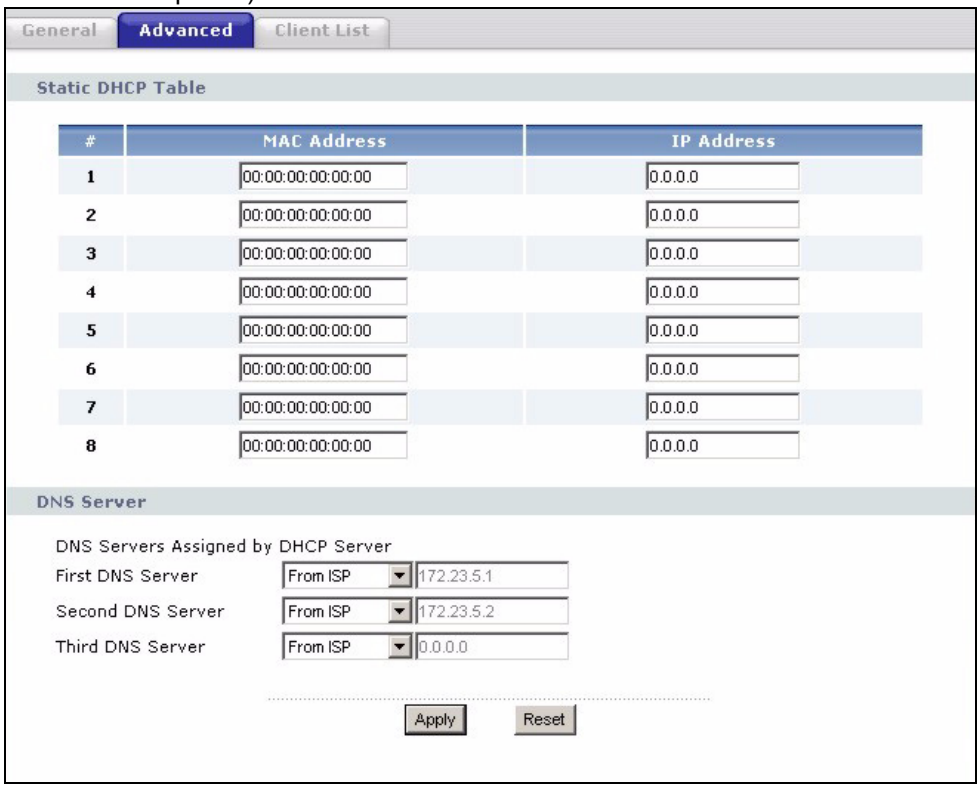
7.3 Окно расширенной настройки сервера DHCP

В этом окне можно назначать IP-адреса отдельным компьютерам локальной сети на основе их MAC-адресов. Здесь же можно указать информацию о сервере DNS, которую NBG334W передает клиентам DHCP.

Каждое устройство Ethernet имеет уникальный MAC-адрес (MAC – Media Access Control – Управление доступом к среде передачи). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

Для изменения в NBG334W статических настроек DHCP, выберите пункт **Network (Сеть) > LAN (Локальная сеть) > Advanced (Дополнительная настройка)**. Появится следующее окно.

Рис. 37 Network (Сеть) > DHCP Server (Сервер DHCP) > Advanced (Дополнительная настройка)



В следующей таблице даны описания полей этого окна.

Табл. 27 Network (Сеть) > DHCP Server (Сервер DHCP) > Advanced (Дополнительная настройка)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер записи в таблице статических IP-адресов (строки).
MAC Address (MAC-адрес)	Введите (через двоеточия) MAC-адрес компьютера локальной сети.
IP Address (IP-адрес)	Введите IP-адрес компьютера локальной сети.
DNS Servers Assigned by DHCP Server (Серверы DNS, назначаемые сервером DHCP) Интернет-центр NBG334WIP-адрес сервера DNS (Domain Name System – система доменных имен) клиентам DHCP (если таковой адрес указан). Интернет-центр NBG334W передает эту информацию только клиентам DHCP локальной сети (если установлен флажок **Enable DHCP Server (Включить сервер DHCP)**). Если флажок **Enable DHCP Server** снят, то для нормальной работы в локальной сети должен быть другой сервер DHCP, иначе для всех компьютеров придется вручную указывать адрес сервера DNS.	

Табл. 27 Network (Сеть) > DHCP Server (Сервер DHCP) > Advanced (Дополнительная настройка)

ПОЛЕ	ОПИСАНИЕ
First DNS Server (Первый сервер DNS) Second DNS Server (Второй сервер DNS) Third DNS Server (Третий сервер DNS)	Выберите вариант **From ISP (Определяется поставщиком Интернет-услуг)**, если Ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN интернет-центра NBG334W). Справа от этого поля отображается (доступный только для чтения) IP-адрес сервера DNS, назначенный поставщиком интернет-услуг. Если Вам известен IP-адрес сервера DNS, выберите вариант **User-Defined (Определяется пользователем)**. Введите этот адрес в поле справа от данного поля. Если выбрать вариант **User-Defined (Определяется пользователем)**, но не указать IP-адрес, то при нажатии на кнопку **Apply (Применить)** вариант **User-Defined** сменится на **None (Отключить)**. Если для второго сервера выбрать вариант **User-Defined (Определяется пользователем)** и указать точно такой же адрес, то при нажатии на кнопку **Apply (Применить)** он поменяется на **None (Нет)**. Чтобы интернет-центр NBG334W мог выполнять функции proxy-сервера DNS, выберите вариант **DNS Relay (Ретрансляция DNS)**. IP-адрес NBG334W в локальной сети отображается в поле справа (только для чтения). В этом случае интернет-центр NBG334W сообщает клиентам DHCP в локальной сети, что роль сервера DNS выполняет NBG334W. Когда компьютер, находящийся в локальной сети, отправляет DNS-запрос интернет-центру NBG334W, NBG334W перенаправляет его на сервер DNS системы NBG334W (настраивается в окне **WAN (Глобальная сеть) > Internet Connection (Подключение к сети Интернет)**) и транслирует ответ обратно на компьютер. Вариант **DNS Relay (Ретрансляция DNS)** можно выбрать только для одного из трех серверов; в противном случае, если выбрать **DNS Relay** для второго или третьего сервера DNS, то после нажатия на кнопку **Apply (Применить)**, он изменится на **None (Нет)**. Если Вы не хотите настраивать серверы DNS, выберите вариант **«None»**. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

7.4 Список клиентов

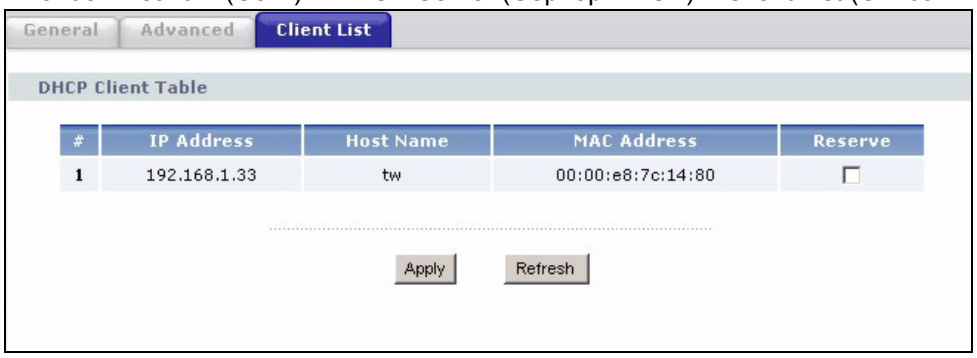
В таблице DHCP отображается текущая информация о клиентах DHCP (включая **IP-адрес**, **имя узла** и **MAC-адрес**) для всех клиентов сети, использующих NBG334W, как сервер DHCP.

Настройте это окно так, чтобы всегда привязывать IP-адрес к MAC-адресу (и имени узла). Выберите пункт **Network (Сеть)** > **DHCP Server (Сервер DHCP)** > **Client List (Список клиентов)**.

Можно также открыть доступный только для чтения список клиентов, щелкнув в окне **Status (Состояние)** ссылку **DHCP Table (Details...) (Таблица DHCP (Подробнее...))**.

Появится следующее окно.

Рис. 38 Network (Сеть) > DHCP Server (Сервер DHCP) > Client List (Список клиентов)



В следующей таблице даны описания полей этого окна.

Табл. 28 Network (Сеть) > DHCP Server (Сервер DHCP) > Client List (Список клиентов)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер узла.
IP Address (IP-адрес)	В этом поле отображается IP-адрес компьютера с номером, указанном выше.
Host Name (Имя узла)	В этом поле отображается имя компьютера.
MAC Address (MAC-адрес)	MAC-адрес (Media Access Control – Управление доступом к среде) или адрес Ethernet в локальной сети является уникальным для каждого компьютера (шесть пар шестнадцатеричных символов). Сетевая интерфейсная карта, такая как Ethernet-адаптер, имеет постоянный адрес, присваиваемый на заводе. Этот адрес отвечает промышленному стандарту, который обеспечивает уникальность этого адреса среди других адаптеров.
Reserve (Резервирование)	Установите этот флажок, чтобы интернет-центр NBG334W всегда привязывал этот IP-адрес к данному MAC-адресу (и имени узла). После нажатия на кнопку **Apply (Применить)**, MAC- и IP-адрес тоже появятся в окне **Advanced (Дополнительная настройка)** (где их можно отредактировать).
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для перезагрузки таблицы DHCP.

8

Трансляция сетевых адресов (NAT)

В этой главе рассказывается, как настроить функцию NAT в NBG334W.

8.1 Общие сведения о NAT

NAT (Network Address Translation – трансляция сетевых адресов, RFC 1631) – это процесс трансляции IP-адресов узла в пакете. Пример трансляции: смена адреса источника исходящего пакета, используемого в одной сети, на IP-адрес в другой сети.

8.2 Применение NAT

Чтобы разрешить прохождение трафика из глобальной сети через NBG334W, необходимо в дополнение к NAT создать правило межсетевого экрана.

8.2.1 Переадресация портов: Службы и номера портов

Набор переадресации портов – это список внутренних серверов (расположенных в локальной сети за NAT), например, web или FTP, которые можно сделать доступными для внешних пользователей, несмотря на то, что NAT представляет всю внутреннюю сеть для внешних пользователей, как одиночный компьютер.

Окно **Application (Приложение)** служит для направления входящих запросов служб на соответствующие сервер(ы) локальной сети. Вы можете указать для переадресации один номер порта или диапазон номеров портов, а также локальный IP-адрес требуемого сервера. Номер порта определяет службу, например, служба web использует порт 80, а FTP – порт 21. В некоторых случаях, когда служба неизвестна или один сервер поддерживает более одной службы (например, FTP и web), лучше указать диапазон номеров портов.

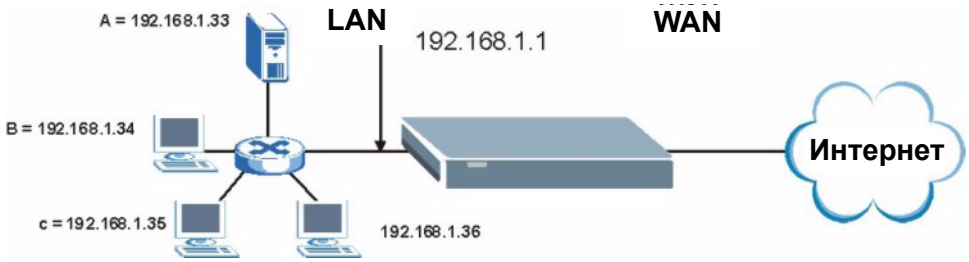
Кроме серверов определенных видов служб NAT поддерживает сервер по умолчанию. Запросы служб без явного указания сервера перенаправляются на стандартный сервер. Если стандартный сервер не задан, запросы просто сбрасываются.

Многие Интернет-провайдеры, предоставляющие широкополосные услуги в жилых районах, не позволяют запускать серверные приложения (такие как Web или FTP сервер) на вашем компьютере. Ваш Интернет-провайдер может периодически делать проверку на наличие серверов и может приостановить действие вашего договора, если обнаружит у вас активные службы. Для прояснения этого вопроса обратитесь к своему Интернет-провайдеру.

8.2.2 Пример настройки серверов, расположенных после преобразования портов

Предположим, вы назначили порты с 21-го по 25-ый одному серверу FTP, Telnet и SMTP (Сервер **A** в примере), порт 80 другому серверу (Сервер **B** в примере) и назначили IP-адрес 192.168.1.35 для стандартного сервера (Сервер **C** в примере). Вы назначили IP-адрес локальной сети, а Интернет-провайдер назначил IP-адрес в глобальной сети. Сеть с NAT из сети Интернет выглядит как одиночный узел.

Рис. 39 Пример: Несколько серверов расположены за NAT



8.3 Окно общей настройки NAT

Щелкните **Network (Сеть) > NAT** для отображения окна **General (Общая настройка)**.

Рис. 40 Network (Сеть) > NAT > General (Общая настройка)

В следующей таблице даны описания полей этого окна.

Табл. 29 Network (Сеть) > NAT > General (Общая настройка)

ПОЛЕ	ОПИСАНИЕ
Enable Network Address Translation (Включить трансляцию сетевых адресов)	NAT (Network Address Translation – Трансляция сетевых адресов) позволяет выполнять преобразование IP-адреса, используемого внутри одной сети (например, частного IP-адреса, используемого в локальной сети) в другой IP-адрес, известный в другой сети (например, общедоступный IP-адрес, используемый в Интернет). Поставьте флажок в этом поле, чтобы включить NAT.
Default Server Setup (Настройка сервера по умолчанию)	
Default Server (Стандартный сервер)	Кроме серверов определенных видов служб NAT поддерживает сервер по умолчанию. Стандартный сервер принимает пакеты от портов, которые не указаны в окне **Application (Приложение)**. Если **стандартному серверу** не назначен IP-адрес, NBG334W сбрасывает все пакеты, принятые для портов, которые не указаны в окне **Приложение (Application)** или в настройках удаленного управления.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

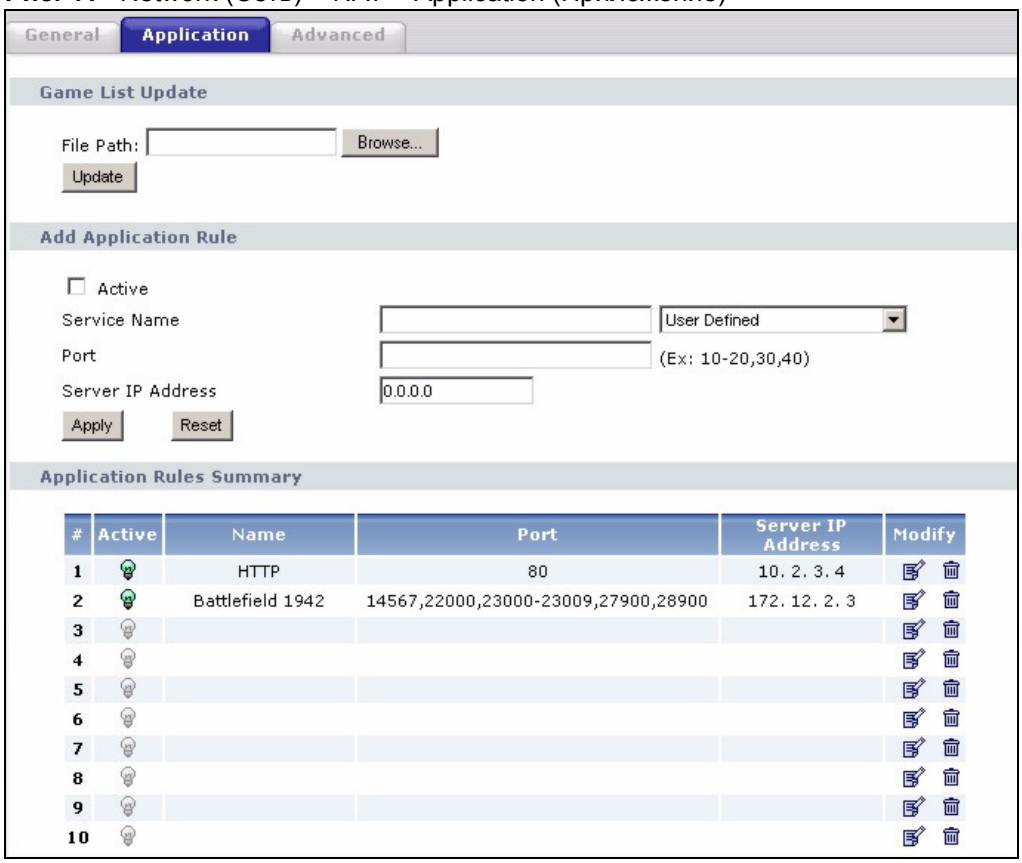
8.4 Окно приложения NAT

Функция переадресации портов позволяет задавать локальные серверы для перенаправления на них входящих запросов служб. Для изменения настроек переадресации портов на интернет-центре NBG334W выберите пункт **Network (Сеть)** > **NAT** > **Application (Приложение)**. При этом откроется следующее окно.

Если не указан IP-адрес **стандартного сервера** в окне **NAT > General (Общая настройка)**, интернет-центр NBG334W будет сбрасывать все пакеты, полученные для портов, не указанных в этом окне или в настройках удаленного управления.

Информацию о номерах портов, обычно используемых для конкретных служб, см. в Прил. F на с. 251.

Рис. 41 Network (Сеть) > NAT > Application (Приложение)



В следующей таблице даны описания полей этого окна.

Табл. 30 Применение NAT

ПОЛЕ	ОПИСАНИЕ
Game List Update (Обновить список игр)	В список игр входят названия стандартных служб и номера портов. Этот список можно изменить и загрузить в интернет-центр NBG334W, чтобы заменить существующие записи во втором поле после **названий служб** (поле **Service Name**).
File Path (Путь к файлу)	Введите путь к файлу, который вы хотите загрузить, или нажмите кнопку **Browse... (Обзор...)**, чтобы указать его местонахождение.
Browse... (Обзор...)	Нажмите кнопку **Browse (Просмотр)**,чтобы указать местонахождение файла с расширением .txt, который вы хотите загрузить. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Update (Обновить)	Нажмите кнопку **Update (Обновить)** для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.
Add Application Rule (Добавление правила приложения)	
Active (Активировать)	Установите этот флажок для включения правила, чтобы запрашиваемая служба могла быть перенаправлена на узел с указанным внутренним IP-адресом. Снимите этот флажок, чтобы запретить переадресацию этих портов на внешний сервер без удаления записи.

Табл. 30 Применение NAT (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service Name (Название службы)	Введите название правила (до 31 печатных символов) в первое поле после поля **Service Name (Название службы)**. В противном случае, выберите стандартную службу во втором поле после **Service Name**. Название стандартной службы и номер(а) порта будут отображены в полях **Service Name (Название службы)** и **Port (Порт)**.
Port (Порт)	Введите сюда номер(а) порта для переадресации. Чтобы указать диапазон портов, введите между первым и последним портом дефис (-), например, 10-20. Чтобы указать два или более непоследовательных порта, разделите их запятой без пробела, например, 123,567.
Server IP Address (IP-адрес сервера)	Введите сюда IP-адрес сервера, получающего пакеты из порта (портов), указанного в поле **Port (Порт)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения в таблице **Application Rules Summary (Сводка правил приложений)**.
Reset (Сброс)	Щелкните **Reset (Сброс)**, чтобы не сохранять изменения и вернуть предыдущие значения в поля **Service Name (Название службы)** и **Port (Порт)**.
Application Rules Summary (Сводка правил приложений)	
#	Номера отдельных записей сервера переадресации портов.
Active (Активировать)	Этот значок активизируется при включении правила.
Name (Имя)	В этом поле отображается название правила.
Port (Порт)	В данном поле отображается номер(а) порта.
Server IP Address (IP-адрес сервера)	В этом поле отображается внутренний IP-адрес сервера.
Modify (Изменить)	Щелкните значок **Edit (Правка)**, чтобы открыть и изменить существующее правило в разделе **Add Application Rule (Добавить правило приложения)**. Для удаления правила щелкните значок **Remove (Удалить)**.

8.4.1 Пример списка игр

В этом разделе приводится пример текстового файла со списком игр. Порядковый номер, название службы и соответствующий порт(ы) указываются через запятую (без пробелов). Для создания новой службы используется формат «name=xxx» (где «xxx» – название службы). Диапазоны портов указываются через дефис (-) (без пробелов). Несколько (непоследовательных) портов могут быть разделены запятыми.

Рис. 42 Пример списка игр

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

8.5 Инициация переадресации портов

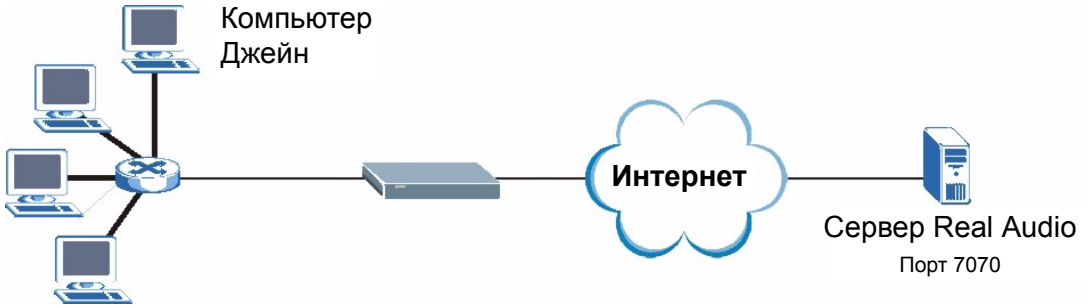
Некоторые службы используют выделенный диапазон портов на клиенте и выделенный диапазон портов на сервере. При обычной переадресации портов в NAT настраивается порт переадресации для перенаправления службы (входящей с сервера глобальной сети) на IP-адрес клиентского компьютера (в локальной сети). Проблема состоит в том, что при переадресации портов служба перенаправляется только на один IP-адрес локальной сети. Чтобы использовать службу на другом компьютере локальной сети, нужно вручную заменить IP-адрес этого компьютера в порту переадресации на IP-адрес другого компьютера этой же сети.

Функция инициации переадресации портов решает эту проблему, позволяя компьютерам локальной сети динамически обмениваться службами. Интернет-центр NBG334W регистрирует IP-адрес компьютера локальной сети, передающего в глобальную сеть запрос на обслуживание с указанием конкретного номера порта и протокола (порта «инициации»). Когда в порт WAN интернет-центра NBG334W поступает ответ с указанием конкретного номера порта и протокола («входящий» порт), NBG334W перенаправляет трафик на IP-адрес компьютера локальной сети, отправившего запрос. После завершения подключения к этому компьютеру, другой компьютер локальной сети может точно также использовать эту службу. Таким образом, не нужно вручную настраивать новый IP-адрес каждый раз, когда другой компьютер локальной сети будет использовать приложение.

8.5.1 Пример инициации переадресации портов

В этом разделе приводится пример инициации переадресации портов.

Рис. 43 Пример процесса инициации переадресации портов



1. Джейн запрашивает файл с сервера Real Audio (порт 7070).
2. Порт 7070 – это порт «инициации» интернет-центра NBG334W на регистрацию IP-адреса компьютера Джейн. NBG334W привязывает этот IP-адрес к диапазону «входящих» портов (6970-7170).
3. Сервер Real Audio отвечает на запрос, указывая порт из диапазона 6970-7170.
4. Интернет-центр NBG334W перенаправляет трафик на IP-адрес компьютера Джейн.
5. Только Джейн сможет работать с сервером Real Audio, пока подключение не будет закрыто (в т.ч. по тайм-ауту). Интернет-центр NBG334W закрывает подключение через три минуты простоя при использовании протокола UDP (User Datagram Protocol – протокол пользовательских дейтаграмм) или через два часа при использовании протокола TCP/IP (Transfer Control Protocol/Internet Protocol – протокол управления передачей/Интернет-протокол).

8.5.2 Два замечания о портах инициации

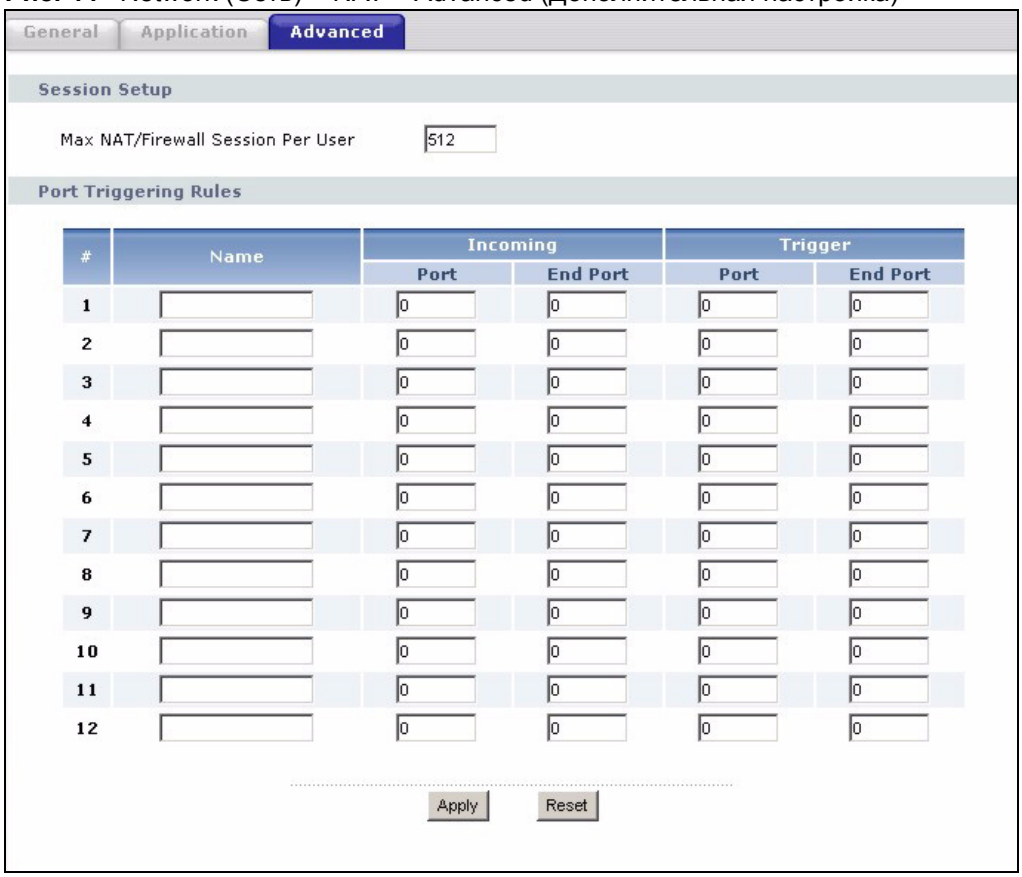
1. Инициация происходит только тогда, когда данные поступают на интернет-центр NBG334W из внутренней сети и предназначены для внешней сети.
2. Если приложение требует непрерывной передачи данных, то соответствующий порт (диапазон) будет занят, и другой компьютер локальной сети не сможет выполнить инициацию.

8.6 Окно расширенной настройки NAT

Для изменения настроек инициации переадресации портов в интернет-центре NBG334W выберите пункт **Network (Сеть) > NAT** > **Advanced (Дополнительная настройка)**. При этом откроется следующее окно.

Одновременно выполнять инициацию может только один компьютер, находящийся в локальной сети.

Рис. 44 Network (Сеть) > NAT > Advanced (Дополнительная настройка)



В следующей таблице даны описания полей этого окна.

Табл. 31 Network (Сеть) > NAT > Advanced (Дополнительная настройка)

ПОЛЕ	ОПИСАНИЕ
Port Triggering Rules (Правила инициации портов)	
#	Это порядковый номер правила (только для чтения).
Name (Имя)	Введите уникальное имя (длиной до 15 символов), которое будет использоваться в целях идентификации. Допускаются любые символы, включая пробелы.
Incoming (Входящий)	Этот порт (или диапазон портов) используется сервером в глобальной сети для отправки определенной службы. Интернет-центр NBG334W перенаправляет трафик с этим портом (или диапазоном портов) на клиентский компьютер локальной сети, отправивший запрос.
Start Port (Начальный порт)	Укажите здесь начало диапазона номеров портов.
End Port (Последний порт)	Укажите здесь конец диапазона номеров портов.
Trigger (Порт инициации)	Порт инициации (диапазон портов) побуждает (инициирует) интернет-центр NBG334W зарегистрировать IP-адрес компьютера локальной сети, отправившего трафик на сервер, расположенный в глобальной сети.

Табл. 31 Network (Сеть) > NAT > Advanced (Дополнительная настройка)

ПОЛЕ	ОПИСАНИЕ
Start Port (Начальный порт)	Укажите здесь начало диапазона номеров портов.
End Port (Последний порт)	Укажите здесь конец диапазона номеров портов.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

9

Динамическая система доменных имен

9.1 Общие сведения о динамической системе доменных имен

Динамическая система доменных имен (DYNDNS) позволяет обновлять ваш текущий динамический IP-адрес с помощью одной или нескольких служб динамических DNS, чтобы любой компьютер мог взаимодействовать с вашим (посредством NetMeeting, CU-SeeMe и т. д.). Вы также можете обеспечить доступ к серверу FTP или Web-сайту на вашем компьютере, с использованием доменного имени (например, myhost.dhs.org, где myhost – имя по вашему выбору), которое остается постоянным, вместо использования IP-адреса, который назначается заново при каждом подключении. Ваши друзья или родственники всегда смогут получить доступ к вашему ресурсу, даже если они не знают точного IP-адреса.

Прежде всего, необходимо получить учетную запись динамической DNS на сайте www.dyndns.org. Эта услуга предназначена для тех, кто использует динамический IP-адрес, назначаемый Интернет-провайдером или сервером DHCP, и кто хотел бы иметь доменное имя. Провайдер услуг динамической DNS предоставляет пароль или ключ.

9.1.1 Шаблоны DYNDNS

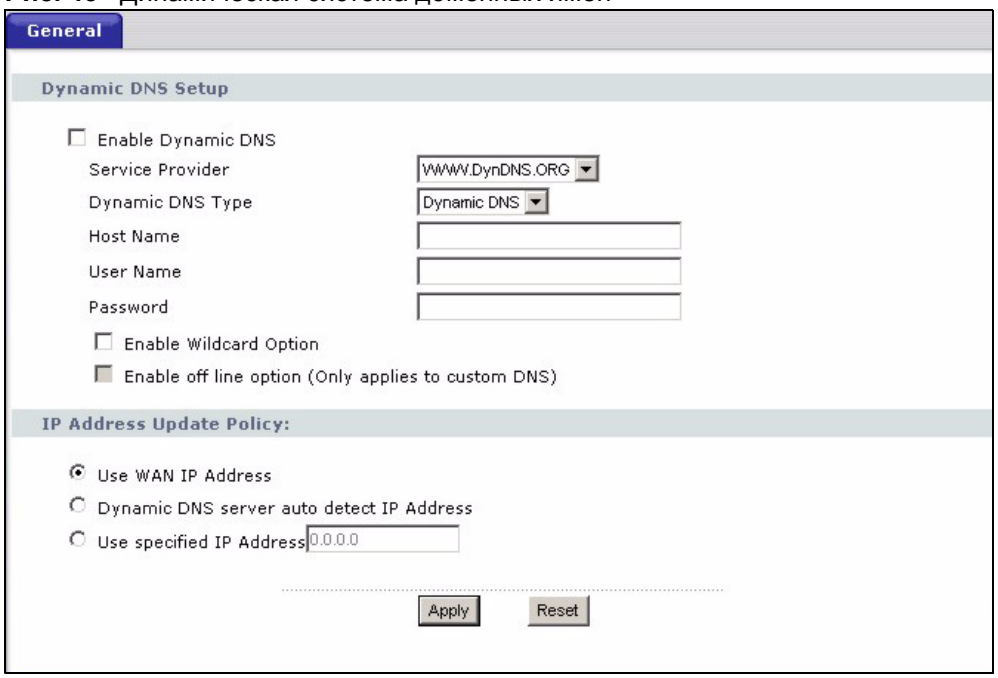
Использование шаблонов позволяет соотносить имена вида *.yourhost.dyndns.org с тем же IP-адресом, что и yourhost.dyndns.org. Данная функция полезна, если вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом предоставлять доступ к вашему узлу.

Если вы имеете частный IP-адрес в глобальной сети, то динамическую DNS использовать нельзя.

9.2 Окно настройки динамической системы доменных имен

Для изменения настроек DDNS на NBG334W выберите пункт **Network (Сеть) > DDNS**. При этом откроется следующее окно.

Рис. 45 Динамическая система доменных имен



В следующей таблице даны описания полей этого окна.

Табл. 32 Динамическая система доменных имен

ПОЛЕ	ОПИСАНИЕ
Enable Dynamic DNS (Включить динамическую систему доменных имен)	Установите этот флажок для использования динамической службы доменных имен.
Service Provider (Провайдер услуг)	В этом можно выбрать поставщика услуг динамической DNS.
Dynamic DNS Type (Тип динамической DNS)	Выберите тип службы, предоставляемой вашим провайдером услуг динамической DNS
Host Name (Имя узла)	Введите в это поле названия узлов. Можно ввести в это поле 2 имени, разделенных запятой («,»).
User Name (Имя пользователя)	Введите Ваше имя пользователя.
Password (Пароль)	Введите назначенный пароль.
Enable Wildcard Option (Включить маску)	Установите этот флажок для включения маски DYNDNS.

Табл. 32 Динамическая система доменных имен

ПОЛЕ	ОПИСАНИЕ
Enable off line option (Включить автономный режим)	Это поле доступно, только если в поле **DDNS Type (Тип DDNS)** установлено **Custom DNS (Пользовательская DNS)**. Проверьте, что провайдер услуг динамической DNS обеспечивает перенаправление трафика на указанный вами URL во время отсутствия подключения к сети.
IP Address Update Policy (Политика обновления IP-адреса):	
Use WAN IP Address (Использовать IP-адрес в глобальной сети)	Выберите эту опцию для обновления IP-адреса для имени узла(ов) на IP-адрес в глобальной сети.
Dynamic DNS server auto detect IP Address (Автоматическое получение IP-адреса от сервера DDNS)	Выберите эту опцию для автоматического обновления IP-адреса для имени узла(ов) с помощью сервера DDNS. Рекомендуется использовать этот вариант.
Use WAN IP Address (Использовать IP-адрес)	Введите IP-адрес для имени узла(ов). Выберите эту опцию, если используется статический IP-адрес.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

Часть III
Безопасность

Межсетевой экран (105)
Фильтрация на основе содержания (113)

10

Межсетевой экран

В данной главе дается вводная информация по межсетевым экранам, а также описывается начало работы с межевым экраном интернет-центра NBG334W.

10.1 Знакомство с межсетевым экраном ZyXEL

10.1.1 Понятие межсетевого экрана

Первоначально термин «firewall» относился к технологии строительства, разработанной в целях предотвращения распространения огня между помещениями. Сетевой термин «firewall» (межсетевой экран) означает систему или группу систем, определяющих политику управления доступом между двумя сетями. Его также можно определить как механизм защиты надежной (в отношении безопасности) сети от ненадежной. Безусловно, межсетевые экраны не решают все проблемы безопасности. Межсетевой экран (другое его название – брандмауэр) – это лишь один из механизмов, предназначенных для создания внешнего периметра защиты сети в рамках политики безопасности сети. Он не должен быть единственным применяемым механизмом или способом. Успешная работа межсетевого экрана возможна только как результат правильной его разработки и установки. Это требует включения межсетевого экрана в общую политику защиты информации. Кроме того, необходимо внедрить определенные политики в рамках собственно межсетевой защиты.

10.1.2 Межсетевой экран с инспекцией пакетов с учетом состояния

Межсетевые экраны с инспекцией пакетов с учетом состояния ограничивают доступ путем отбраковки пакетов, не удовлетворяющих установленным правилам доступа. Решения о доступе принимаются в зависимости от IP-адреса и протокола. Такие межсетевые экраны также «инспектируют» данные сеансов связи для обеспечения целостности соединения и адаптации к динамическим протоколам. Как правило, такие экраны обеспечивают лучшую скорость и прозрачность, однако проигрывают в таких аспектах как управление доступом на уровне приложений и кэширование, которые поддерживаются некоторыми прокси. Межсетевые экраны того или иного типа сегодня являются неотъемлемой частью стандартных решений систем безопасности для предприятий.

10.1.3 Описание межсетевого экрана интернет-центра NBG334W

Межсетевой экран интернет-центра NBG334W относится к типу экранов с инспекцией пакетов с учетом состояния и в активном состоянии предназначен для защиты от атак типа «отказ в обслуживании» (включается на вкладке **General (Общие настройки)** в разделе **Firewall (Межсетевой экран)** установкой флажка в поле **Enable Firewall (Включить межсетевой экран)**). Задачей межсетевого экрана NBG334W является обеспечение безопасного подключения частной локальной сети (LAN) к Интернет. NBG334W также можно использовать для предотвращения несанкционированного копирования, уничтожения и изменения данных или регистрационных журналов, что важно с точки зрения безопасности локальной сети.

Интернет-центр NBG334W включается между локальной сетью и сетью интернет-провайдера. Это позволяет ему выступать в качестве безопасного шлюза для данных, пересылаемых из локальной сети в Интернет и наоборот.

Интернет-центр NBG334W оборудован одним портом Ethernet WAN и четырьмя портами Ethernet LAN, которые физически разделяют сеть на две части. В порт WAN (Wide Area Network – глобальная сеть) подключается выделенная линия Ethernet, обеспечивающая выход в Интернет.

Порт LAN (Local Area Network – локальная сеть) подключается к компьютерной сети, для которой необходимо обеспечить защиту от внешнего мира. Компьютеры сети будут иметь доступ к Интернет-службам, таким как электронная почта, FTP, и WWW. При этом «входящий доступ» будет запрещен (по умолчанию), пока удаленный узел не пройдет авторизацию на использование конкретной службы.

10.1.4 Методы усиления безопасности при помощи межсетевого экрана

1. Измените пароль по умолчанию при помощи Web-конфигуратора.
2. Подумайте о допуске к интернет-центру до его подключения в сеть.
3. Ограничьте круг лиц, имеющих право доступа к маршрутизатору.
4. Не подключайте неиспользуемые локальные службы (SNMP или NTP). Любое такое лишнее подключение может представлять потенциальную угрозу безопасности. Находчивый хакер может отыскать оригинальные способы злоупотребления подключенными службами для получения доступа к межсетевому экрану или сети.
5. Подключенные локальные серверы необходимо обезопасить. Защита обеспечивается путем ограничения взаимодействия до конкретных клиентских устройств и назначения правил блокировки пакетов, поступающих через конкретный интерфейс.
6. Активированный межсетевой экран обеспечит защиту от подмены IP-адресов.
7. Само устройство межсетевого экрана должно находиться в недоступном (закрытом) помещении.

10.2 Треугольные маршруты

Если в локальной сети имеется шлюз с IP-адресом, входящим в ту де подсеть, что и NBG334W, то обратный трафик может и не проходить через NBG334W. Такой маршрут называется асимметричным или «треугольным». В результате NBG334W сбрасывает соединение, так как для этого соединения отсутствует подтверждение.

Можно настроить NBG334W на работу с асимметричными маршрутами (чтобы он не разрывал подключение).

Использование несимметричных маршрутов может привести к передаче трафика из глобальной сети прямо к компьютеру локальной сети без прохождения через маршрутизатор NBG334W. Лучше воспользоваться псевдонимом IP, чтобы поместить NBG334W и резервный шлюз в разные подсети.

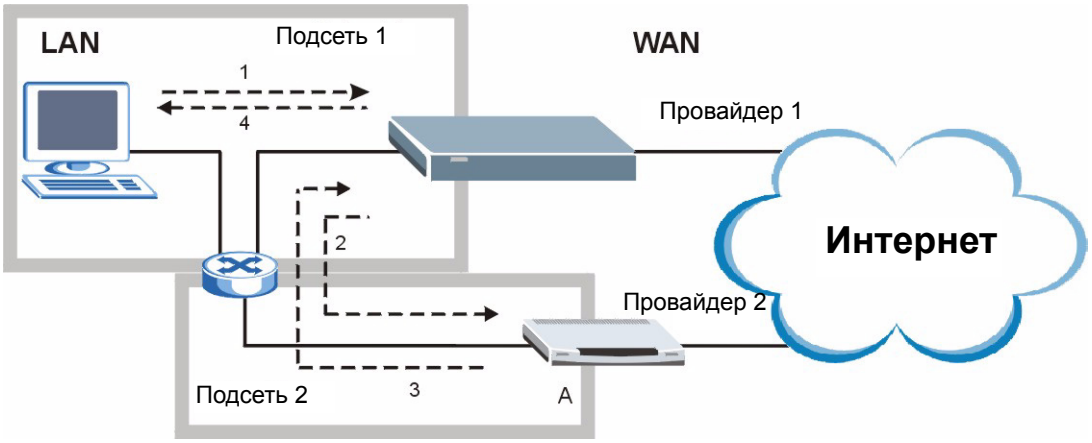
10.2.1 Треугольные маршруты и псевдоним IP

Чтобы не допускать треугольных маршрутов, можно использовать псевдоним IP. Псевдоним IP позволяет разделить локальную сеть на несколько логических сегментов с использованием одного интерфейса.

При расположении локальной сети и шлюза «**A**» в разных подсетях весь сетевой трафик, возвращающийся в локальную сеть, должен проходить через NBG334W. Это можно представить с помощью следующего сценария.

1. Компьютер локальной сети инициирует соединение, посылая пакет SYN принимающему серверу в глобальной сети.
2. Маршрутизатор NBG334W изменяет маршрут пакета и отправляет его на шлюз **A**, который находится в **подсети 2**.
3. Ответ из глобальной сети приходит на NBG334W.
4. Затем NBG334W перенаправляет его на компьютер, который находится в **подсети 1**.

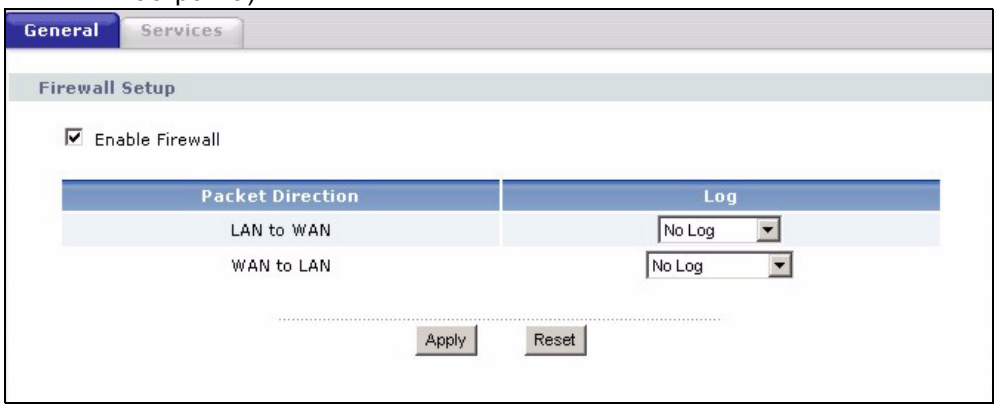
Рис. 46 Использование псевдонима IP для решения проблемы треугольного маршрута



10.3 Окно общей настройки межсетевого экрана

Щелкните **Security (Безопасность) > Firewall (Межсетевой экран)** для отображения окна **General (Общая настройка)**. В этом окне можно включить или отключить межсетевой экран NBG334W и настроить протоколирование его работы.

Рис. 47 Security (Безопасность) > Firewall (Межсетевой экран) > General (Общая настройка)



В следующей таблице даны описания полей этого окна.

Табл. 33 Security (Безопасность) > Firewall (Межсетевой экран) > General (Общая настройка)

ПОЛЕ	ОПИСАНИЕ
Enable Firewall (Включить межсетевой экран)	Выберите эту опцию, чтобы включить межсетевой экран. Если межсетевой экран включен, NBG334W осуществляет управление доступом и защиту от атак типа «Отказ в обслуживании» (DoS).
Packet Direction (Направление пакетов)	Здесь задается направление движения пакетов. Правила межсетевого экрана группируются по направлениям движения пакетов, к которым они применяются.
Log (Регистра-ционный журнал)	Эта опция позволяет включить протоколирование движения пакетов при их блокировании или перенаправлении. Чтобы разрешить протоколирование пакетов, обрабатываемых правилами межсетевого экрана, убедитесь, что в окне **Logs (Журналы)** > **Log Settings (Настройка журналов)** в разделе **Log (Журнал)** выбран вариант **Access Control (Контроль доступа)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

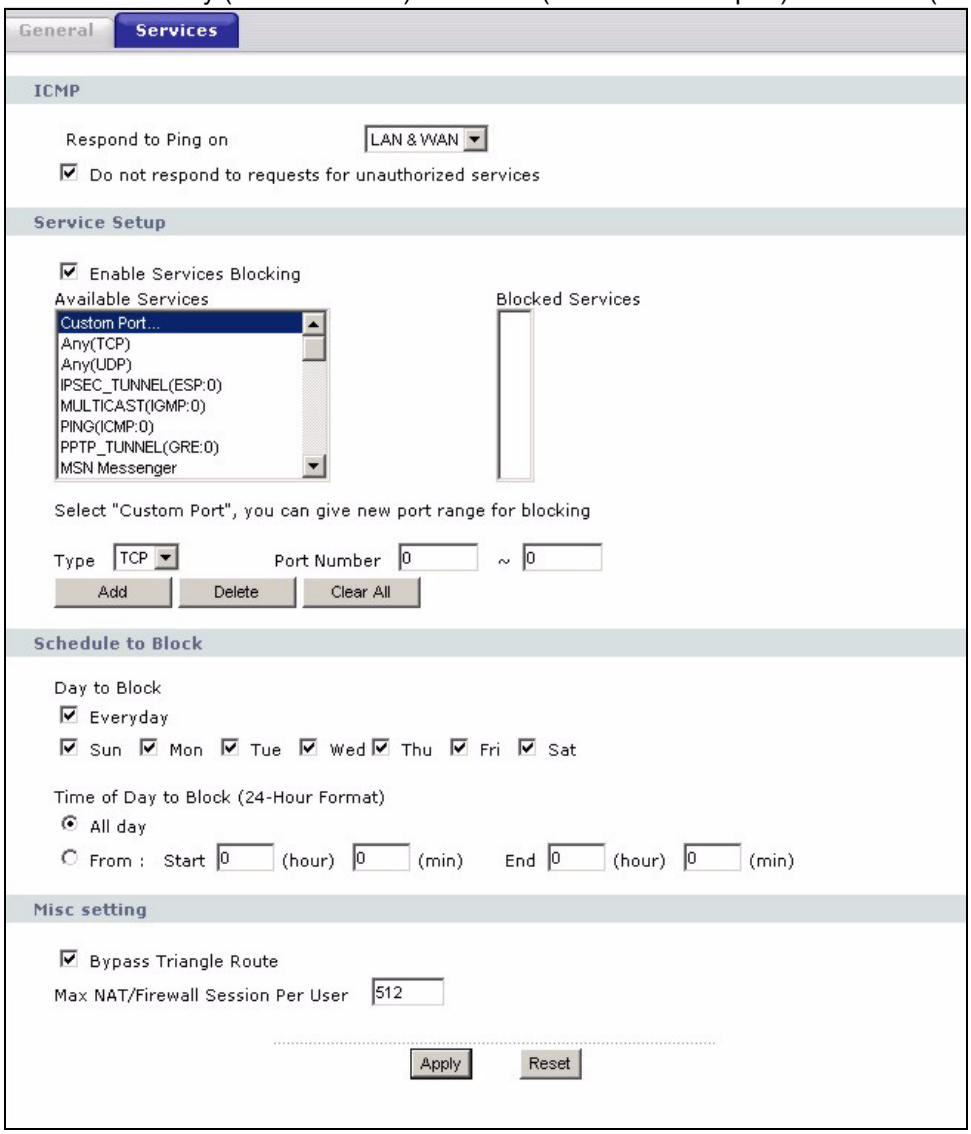
10.4 Окно служб

Выберите пункт **Security (Безопасность) > Firewall (Межсетевой экран) > Services (Службы)**. Появляется окно, как показано ниже.

Если внешний пользователь попытается прозондировать неподдерживаемый порт NBG334W, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании интернет-центра NBG334W. В этом окне можно запретить отправку ответного пакета ICMP. Это позволяет скрыть существование NBG334W от посторонних лиц при попытке зондирования неподдерживаемого порта.

Это окно позволяет также включить блокировку служб, добавить, удалить или изменить подлежащие блокированию службы, а также задать время их блокировки.

Рис. 48 Security (Безопасность) > Firewall (Межсетевой экран) > Services (Службы)



В следующей таблице даны описания полей этого окна.

Табл. 34 Security (Безопасность) > Firewall (Межсетевой экран) > Services (Службы)

ПОЛЕ	ОПИСАНИЕ
ICMP	Протокол управляющих сообщений в сети Интернет (Internet Control Message Protocol) является протоколом управляющих сообщений и сообщений об ошибках между основным узлом и шлюзом в Интернет. ICMP использует дейтаграммы Интернет-протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP и невидимы для пользователей приложений.
Respond to PING on (Отвечать на PING-запросы)	Интернет-центр NBG334W не отвечает на входящие запросы эхо-тестирования, если в поле **Disable (Отключить)** установлен флажок. Выберите **LAN** для ответа на входящие Ping-запросы из локальной сети.Выберите **WAN** для ответа на входящие Ping-запросы из глобальной сети. В противном случае выберите **«LAN & WAN»** для ответа на Ping-запросы как по локальной, так и глобальной сети.
Do not respond to requests for unauthorized services (Не отвечать на запросы для несанкционированных служб).	Установите флажок, чтобы предотвратить обнаружение хакерами интернет-центра NBG334W посредством зондирования неиспользуемых портов. Если флажок установлен, NBG334W не будет отвечать на запросы на неиспользуемые порты. Таким образом, неиспользуемые порты и интернет-центр NBG334W остаются невидимыми. По умолчанию флажок снят и NBG334W посылает пакет ICMP «Port Unreachable» (Порт недоступен) в ответ на зондирование неиспользуемых портов UDP, а в ответ на зондирование неиспользуемых портов TCP – пакет «TCP Reset» (Сброс TCP). Следует отметить, что прежде чем зондирующие пакеты достигнут механизма блокирования эхо-тестирования, они сначала должны пройти через межсетевой экран NBG334W. Поэтому если механизм межсетевого экрана заблокирует зондирующий пакет, то интернет-центр NBG334W отреагирует в зависимости от политики межсетевого экрана, которая по умолчанию отправляет пакет сброса TCP для заблокированного пакета TCP. Для изменения этой политики Вы можете использовать команду «sys firewall tcprst rst [on|off]». Когда механизм межсетевого экрана блокирует пакет UDP, он удаляет его, не отправляя ответного пакета.
Service Setup (Настройка служб)	
Enable Services Blocking (Включить блокировку служб)	Поставьте флажок в этом поле для включения функции.
Available Services (Доступные службы)	В этом списке содержатся службы (порты), использование которых компьютерами локальной сети можно запретить. Выберите блокируемый порт из выпадающего списка и нажмите **Add (Добавить)**, чтобы добавить его в поле **Blocked Services (Блокированные службы)**.
Blocked Services (Заблокированные службы)	В этом списке содержатся службы (порты), недоступные компьютерам локальной сети при включенной функции блокирования служб.
Custom Port (Собственный порт)	Собственный порт настраивается пользователем и отсутствует в списке **Available Services (Доступные службы)**; для его настройки необходимо заполнить два следующих поля.
Type (Тип)	Выберите из выпадающего списка порт IP (**TCP** или **UDP**) для собственного порта.
Port Number (Номер порта)	Укажите для службы диапазон портов. Например, для определения службы Gnutella, выберите тип **TCP** и укажите диапазон портов от 6345 до 6349.

Табл. 34 Security (Безопасность) > Firewall (Межсетевой экран) > Services (Службы)

ПОЛЕ	ОПИСАНИЕ
Add (Добавить)	Выберите службу из выпадающего списка **Available Services (Доступные службы)** и нажмите кнопку **Add (Добавить)**, чтобы добавить службу в список блокированных (**Blocked Services**).
Delete (Удалить)	Выберите службу из списка **Blocked Services (Блокированные службы)** и нажмите кнопку **Delete (Удалить)**, чтобы удалить ее из списка.
Clear All (Очистить все)	Нажмите кнопку **Clear All (Очистить все)**, чтобы очистить список **Blocked Services (Блокированные службы)**.
Schedule to Block (График блокирования)	
Day to Block (Дни блокирования)	Поставьте галочку в этом поле, чтобы задать, в какие дни недели (или каждый день) необходимо блокировать службу.
Time of Day to Block (24-Hour Format) (Время блокирования в 24-часовом формате)	Выберите время блокирования службы. Выбрав вариант **All Day (Весь день)**, можно заблокировать службу на целый день. Можно указать период блокирования, выбрав вариант **From (C)** и введя время начала в поля **Start (hour) (Час начала)** и **Start (min) (Минута начала)** и в поля **End (hour) (Час окончания)** и **End (min) (Минута окончания)**. Время следует указывать в 24-часовом формате, например, вместо «3:00pm» нужно вводить «15:00».
Misc setting (Разные настройки)	
Bypass Triangle Route (Обходной треугольный маршрут)	Поставьте в этом поле флажок, чтобы межсетевой экран NBG334W игнорировал использование треугольной топологии маршрутов в сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

11

Фильтрация на основе содержания

В этой главе кратко рассматривается фильтрация на основе содержания с использованием расширенного графического веб-интерфейса пользователя.

11.1 Введение в фильтрацию на основе содержания

Фильтрация информации, поступающей из сети Интернет, позволяет создавать и реализовывать правила доступа в Интернет, настроенные под конкретные потребности. Фильтрация на основе содержания позволяет блокировать определенные веб-функции или URL-адреса по указанным ключевым словам.

11.2 Ограничение веб-функций

Интрнет-центр NBG334W может блокировать такие функции, как элементы управления ActiveX, Java-апплеты, cookies, а также отключать веб-прокси.

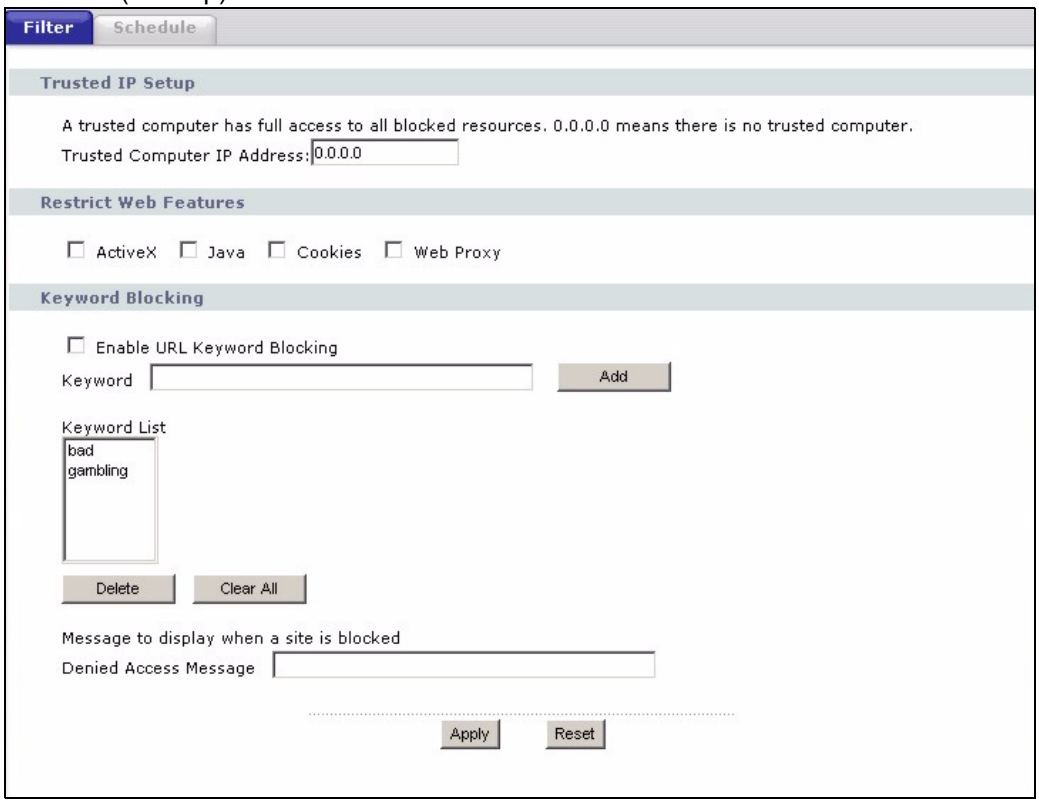
11.3 График блокирования

Интернет-центр NBG334W также позволяет задавать временные периоды, в течение которых NBG334W будет выполнять фильтрацию на основе содержания.

11.4 Окно фильтра

Выберите пункт **Security (Безопасность)** > **Content Filter (Фильтр на основе содержания)**, чтобы открыть окно **Filter (Фильтр)**.

Рис. 49 Security (Безопасность) > Content Filter (Фильтр на основе содержания) > Filter (Фильтр)



В следующей таблице даны описания полей этого окна.

Табл. 35 Security (Безопасность) > Content Filter (Фильтр на основе содержания) > Filter (Фильтр)

ПОЛЕ	ОПИСАНИЕ
Trusted Computer IP Address (IP-адрес надежного компьютера)	Для включения этой функции введите IP-адрес одного из компьютеров Вашей сети, который Вы хотите пометить, как надежный. Этот компьютер будет иметь полный доступ ко всем заблокированным фильтром функциям. Можно оставить это поле пустым, если Вы не хотите указывать надежный компьютер.
Restrict Web Features (Ограничить веб-функции)	Для отключения функции, поставьте напротив нее флажок (флажки). При загрузке страницы, содержащей ограниченную функцию, на ее месте либо ничего не будет, либо это место будет затенено.
ActiveX	Это инструмент для построения динамических и активных веб-страниц, а также приложений с распределенными объектами. При загрузке веб-сайта с элементом ActiveX, он загружается браузером и хранится в системе на случай повторной загрузки страницы.
Java	Это язык и среда программирования для создания загружаемых веб-компонентов и деловых Интернет- или интранет-приложений всех видов.
Cookies	Используются веб-серверами для отслеживания использования их служб, предоставляемых по конкретным идентификаторам.
Web Proxy	Этот сервер играет роль посредника между пользователем и сетью Интернет, обеспечивая безопасность подключений, административный контроль и кэширование. Если такой сервер установлен в глобальной сети, то пользователи локальной сети могут обойти фильтрацию на основе содержания, указав на него.

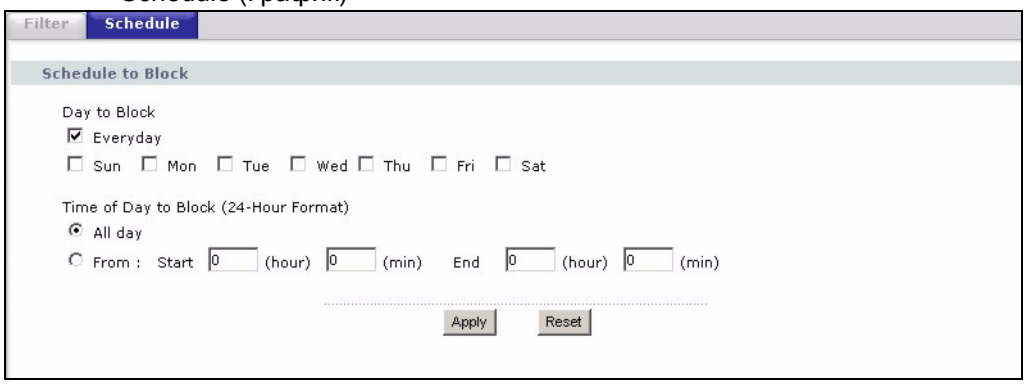
Табл. 35 Security (Безопасность) > Content Filter (Фильтр на основе содержания) > Filter (Фильтр)

ПОЛЕ	ОПИСАНИЕ
Keyword Blocking (Блокирование ключевых слов)	
Enable URL Keyword Blocking (Включить блокировку URL-адресов по ключевым словам)	Интернет-центр NBG334W может блокировать веб-сайты, URL-адреса которых содержат определенные ключевые слова в доменных именах или IP-адресах. Например, если в качестве ключевого слова задать «bad», то будут блокированы все сайты, у которых это слово содержится в доменном имени или IP-адресе (например, сайт http://www.website.com/bad.html будет заблокирован). Поставьте флажок в этом поле для включения функции.
Keyword (Ключевое слово)	Введите в это поле ключевое слово. Допускается использование любых символов (до 64 символа). Использование знаков препинания не допускается. Можно также указать числовой IP-адрес.
Keyword List (Список ключевых слов)	Этот список содержит уже добавленные ключевые слова.
Add (Добавить)	Нажмите кнопку **Add (Добавить)** после ввода ключевого слова. Повторите эту процедуру, если нужно добавить другие ключевые слова. Допускается до 64 ключевых слов. При попытке доступа к web-странице, содержащей ключевое слово, будет выведено сообщение о том, что контент-фильтр заблокировал запрос.
Delete (Удалить)	Выделите ключевое слово в нижнем списке и нажмите **Delete (Удалить)**, чтобы удалить его. После нажатия кнопки **Apply (Применить)** это слово исчезнет из списка.
Clear All (Очистить все)	Нажмите эту кнопку, чтобы удалить все ключевые слова.
Denied Access Message (Сообщение об отказе в доступе)	Введите сюда сообщение, которое должен получать пользователь при попытке доступа к запрещенному веб-сайту. По умолчанию используется сообщение «Please contact your network administrator!» (Пожалуйста, обратитесь к администратору сети!)
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

11.5 График

В этом окне можно настроить график фильтрации интернет-центром NBG334W веб-сайтов на основе из содержания. Выберите пункт **Security (Безопасность)** > **Content Filter (Фильтрация на основе содержания)** > **Schedule (График)**. Появится следующее окно.

Рис. 50 Security (Безопасность) > Content Filter (Фильтр на основе содержания) > Schedule (График)



В следующей таблице даны описания полей этого окна.

Табл. 36 Security (Безопасность) > Content Filter (Фильтр на основе содержания) > Schedule (График)

ПОЛЕ	ОПИСАНИЕ
Day to Block: (Дни блокирования:)	Выберите дни, в которые интернет-центр NBG334W должно выполнять фильтрацию на основе содержания. Чтобы выбрать все дни, поставьте флажок в поле **Everyday (Каждый день)**.
Time of Day to Block (24-Hour Format) (Время блокирования в 24-часовом формате)	Поле **Time of Day to Block (Время блокирования)** позволяет администратору задать временные периоды фильтрации на основе содержания. Значение поля **Time of Day to Block** касается только ограничения по ключевым словам (см. выше). Оно не действует на функции веб-серверов, например, на элементы ActiveX, Java, Cookies и Web Proxy. Для включения постоянной фильтрации в дни, указанные в поле **Day to Block (Дни блокирования)** выберите вариант **All Day (Весь день)**. Чтобы указать период фильтрации на основе содержания, выберите вариант **From (C)** и введите период времени в 24-часовом формате.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

11.6 Настройка блокирования URL-адресов по ключевым словам

С помощью команд можно настроить область URL-адреса, которая будет проверяться на наличие в ней ключевых слов. Информацию по использованию интерпретатора команд см. в приложениях.

11.6.1 Проверка URL-адреса по доменному имени или IP-адресу

По умолчанию, интернет-центр NBG334W проверяет доменное имя или IP-адрес URL на наличие в нем ключевых слов для последующего его блокирования.

Это значит, что NBG334W проверяет символы в URL до первого слэша.

Пример: в адресе www.zyxel.com.tw/news/pressroom.php поиск выполняется только в строке www.zyxel.com.tw.

11.6.2 Полная проверка URL-адреса

При полной проверке URL-адресов интернет-центр NBG334W ищет ключевые слова до последнего слэша.

Пример: в адресе www.zyxel.com.tw/news/pressroom.php поиск выполняется в строке www.zyxel.com.tw/news/.

Для расширения (или сокращения) области поиска в URL-адресе используйте команду `ip urlfilter customize actionFlags 6 [disable | enable]`.

11.6.3 Проверка URL-адреса по имени файла

При проверке URL-адреса по имени файла интернет-центр NBG334W проверяет все символы в URL.

Пример: в адресе www.zyxel.com.tw/news/pressroom.php будут проверяться все символы.

Для расширения (или сокращения) области поиска в URL-адресе используйте команду `ip urlfilter customize actionFlags 8 [disable | enable]`.

Часть IV
Управление

Окна настройки статических маршрутов (121)
Управление пропускной способностью (125)
Удаленное управление (139)
Универсальная функция Plug and Play (UPnP) (145)

12

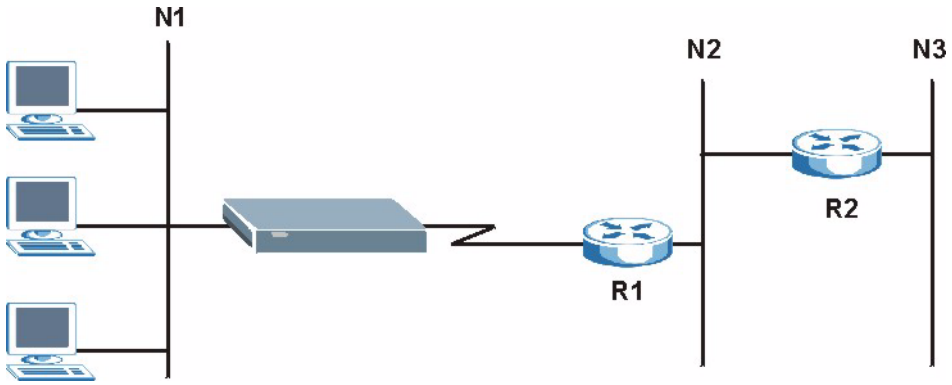
Окна настройки статических маршрутов

В этой главе рассказывается о настройке статических маршрутов NBG334W.

12.1 Обзор статических маршрутов

Каждый удаленный узел определяет только ту сеть, к шлюзу которой он непосредственно подключается. Аналогично и NBG334W не имеет никакой информации о сетях, находящихся за ним. В примере на следующем рисунке NBG334W получает информацию о сети **N2** от маршрутизатора **R1** удаленного узла. Несмотря на это, NBG334W не может отправить пакет в сеть **N3**, поскольку он не «знает» о маршруте, пролегающем через тот же маршрутизатор **R1** удаленного узла (через маршрутизатор-шлюз **R2**). Статические маршруты предназначены для того, чтобы предоставлять NBG334W информацию о сетях за пределами удаленных узлов.

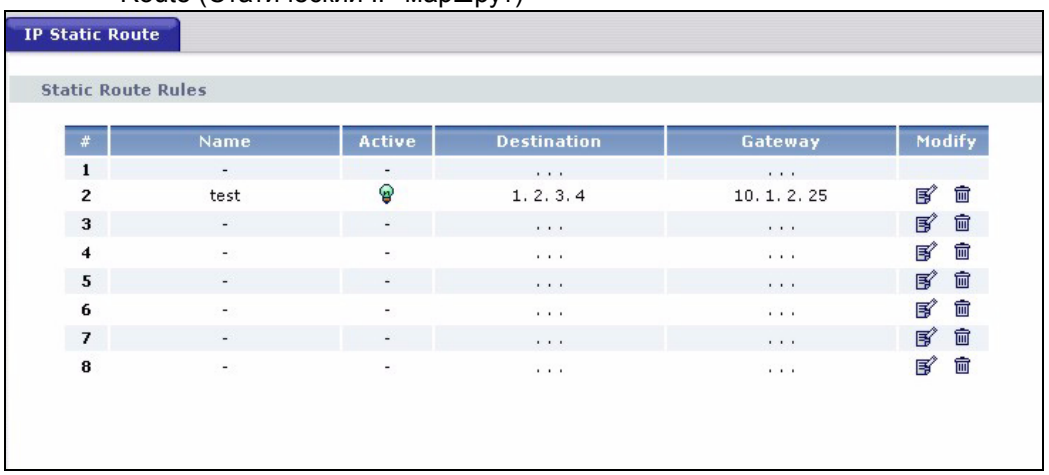
Рис. 51 Пример топологии статической маршрутизации



12.2 Окно настройки статического IP-маршрута

Щелкните **Management (Управление) > Static Route (Статический маршрут)** для отображения окна **IP Static Route (Статический IP-маршрут)**. Появится следующее окно.

Рис. 52 Management (Управление) > Static Route (Статический маршрут) > IP Static Route (Статический IP-маршрут)



В следующей таблице даны описания полей этого окна.

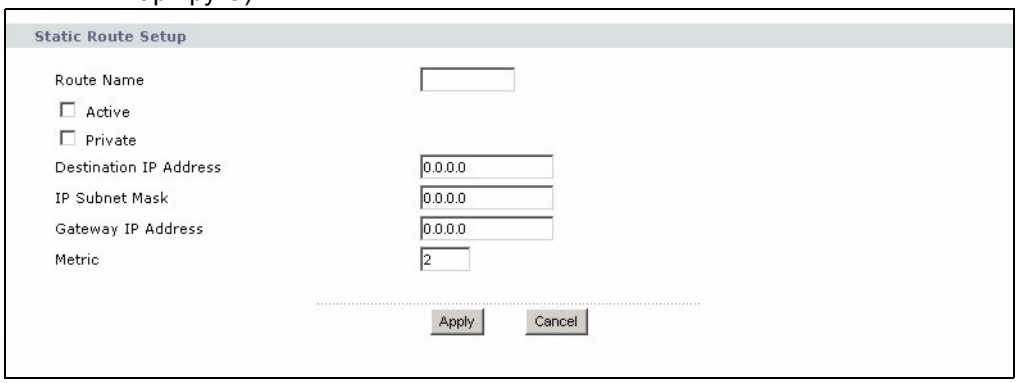
Табл. 37 Management (Управление) > Static Route (Статический маршрут) > IP Static Route (Статический IP-маршрут)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер конкретного маршрута. Первая запись здесь – стандартный маршрут, который не редактируется.
Name (Имя)	Это описательное имя данного маршрута.
Active (Активен)	Этот значок появляется, когда статический маршрут становится активным. Чтобы активизировать маршрут, щелкните значок **Edit (Правка)** в поле **Modify (Изменить)** и поставьте флажок **Active (Активен)** в окне **Static Route Setup (Настройка статического маршрута)**. Чтобы исключить маршрут, не удаляя его, снимите этот флажок.
Destination (Получатель)	Данный параметр определяет сетевой IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе номера сети.
Gateway (Шлюз)	В этом поле отображается IP-адрес шлюза. Шлюз – это непосредственный сосед интернет-центра NBG334W, который будет перенаправлять пакеты получателю. В локальной сети роль шлюза выполняет маршрутизатор, который должен находиться в том же сегменте, что и NBG334W; в глобальной сети в качестве шлюза указывается IP-адрес одного из удаленных узлов.
Modify (Изменить)	Щелкните значок **Edit (Правка)** для перехода к окну настройки статического маршрута. В этом окне можно изменить **статический маршрут** или создать новый. Для удаления маршрута щелкните значок **Remove (Удалить)**.

12.2.1 Окно настройки статического маршрута

Для изменения статического маршрута щелкните значок редактирования в поле **Modify (Изменить)**. Появится следующее окно. Введите в нем необходимую информацию по каждому из маршрутов.

Рис. 53 Management (Управление) > Static Route (Статический маршрут) > IP Static Route: Static Route Setup (Статический IP-маршрут: настройка статического маршрута)



В следующей таблице даны описания полей этого окна.

Табл. 38 Management (Управление) > Static Route (Статический маршрут) > IP Static Route: Static Route Setup (Статический IP-маршрут: настройка статического маршрута)

ПОЛЕ	ОПИСАНИЕ
Route Name (Имя маршрута)	Введите имя статического маршрута IP. Чтобы удалить данный статический маршрут, оставьте это поле пустым.
Active (Активировать)	Это поле позволяет включать/выключать статический маршрут.
Private (Частный адрес)	Этот параметр определяет, будет ли NBG334W включать маршрут к этому удаленному узлу в свою широковещательную рассылку RIP. Отметьте этот флажок, чтобы оставить этот маршрут частным и не включать его в широковещательную рассылку RIP. Снимите флажок, чтобы распространить этот маршрут по другим узлам через широковещательную рассылку RIP.
Destination IP Address (IP-адрес получателя)	Данный параметр определяет сетевой IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе номера сети. Если нужно определить маршрут к одиночному узлу, в поле маски подсети используйте маску подсети 255.255.255.255, чтобы номер сети и адрес узла были одинаковыми.
IP Subnet Mask (IP-маска подсети)	Введите маску подсети IP.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюз – это непосредственный сосед интернет-центра NBG334W, который будет перенаправлять пакеты получателю. В локальной сети роль шлюза выполняет маршрутизатор, который должен находиться в том же сегменте, что и NBG334W; в глобальной сети в качестве шлюза указывается IP-адрес одного из удаленных узлов.
Metric (Метрика)	Метрика определяет «стоимость» передачи и используется для целей маршрутизации. При маршрутизации IP в качестве единицы «стоимости» используется счетчик переходов по сети, при этом минимальное значение «стоимости» равно 1 и соответствует прямому соединению между сетями. Введите число, которое будет приблизительно выражать «стоимость» трафика для данного канала. Число не обязательно должно быть точным, но должно находиться в диапазоне от 1 до 15. В большинстве случаев хорошо подходит значение 2 или 3.

Табл. 38 Management (Управление) > Static Route (Статический маршрут) > IP Static Route: Static Route Setup (Статический IP-маршрут: настройка статического маршрута)

ПОЛЕ	ОПИСАНИЕ
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения настроек NBG334W.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для возврата к предыдущему окну без сохранения изменений.

13

Управление пропускной способностью

В этой главе рассказывается о настройке управления пропускной способностью NBG334W, изменении правил и просмотре регистрационных журналов управления пропускной способностью.

13.1 Обзор управления пропускной способностью

Управление пропускной способностью ZyXEL позволяет устанавливать правила управления пропускной способностью для отдельных приложений и/или подсетей. В правилах можно устанавливать определенную величину пропускной способности (бюджет).

Управление пропускной способностью применяется к трафику, выходящему через интерфейс NBG334W. NBG334W не управляет пропускной способностью входящего трафика.

Управление пропускной способностью применяется ко всему трафику, выходящему через порт маршрутизатора, независимо от источника этого трафика.

Перенаправление трафика и псевдонимы IP могут вызвать трафик между локальными сетями, который проходит через NBG334W, и следовательно, регулируется системой управления пропускной способностью.

- Сумма долей пропускной способности, которые применяются к интерфейсу WAN (из LAN в WAN, из WLAN в WAN, из WAN в WAN / NBG334W) не должна превышать **исходящей пропускной способности**, заданной в окне **Bandwidth Management Advanced (Расширенное управление пропускной способностью)**.
- Сумма долей пропускной способности, применяемых к порту LAN (из WAN в LAN, из WLAN в LAN, из LAN в LAN / NBG334W) не должна превышать 100 000 Кбит/с (Вы не можете настроить баланс пропускной способности для порта LAN).
- Сумма долей пропускной способности, применяемых к порту WLAN (из LAN в WLAN, из WAN в WLAN, из WLAN в WLAN / NBG334W) не должна превышать 54 000 Кбит/с (Вы не можете настроить баланс пропускной способности для порта WLAN).

13.2 Управление пропускной способностью на основе приложений

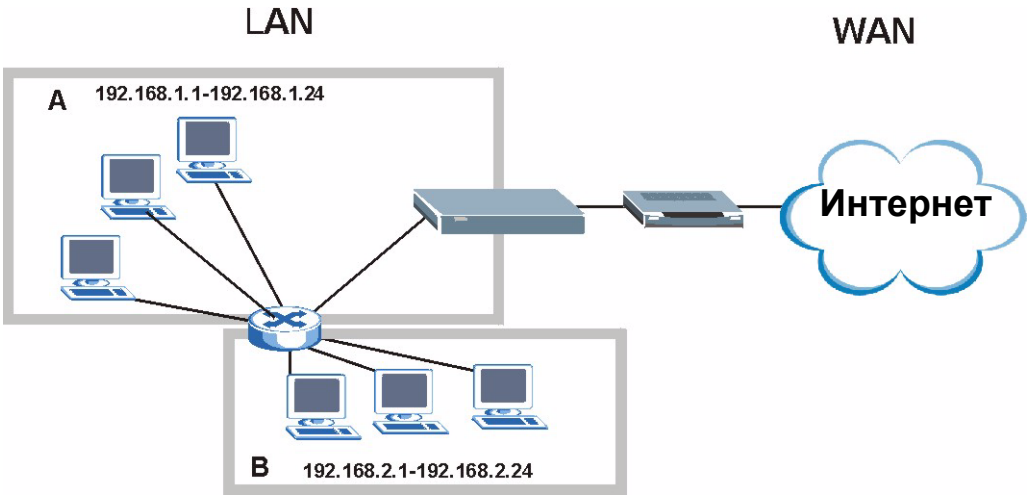
Вы можете создавать классы пропускной способности на основе конкретных приложений (например, VoIP, Web, FTP, E-mail и передача видеосигналов).

13.3 Управление пропускной способностью на основе подсетей

Вы можете создавать классы пропускной способности на основе подсетей.

На следующем рисунке показаны локальные подсети. Можно установить один класс пропускной способности для подсети **A**, а другой – для подсети **B**.

Рис. 54 Пример управления пропускной способностью на основе подсети



13.4 Управление пропускной способностью на основе приложений и подсетей

Также можно создавать классы пропускной способности на основе комбинирования подсетей и приложений. В следующей таблице приводится пример распределения пропускной способности для трафика конкретных приложений из разных локальных подсетей.

Табл. 39 Пример управления пропускной способностью на основе приложения и подсети

ТИП ТРАФИКА	ИЗ ПОДСЕТИ A	ИЗ ПОДСЕТИ B
VoIP	64 Кбит/с	64 Кбит/с
Web	64 Кбит/с	64 Кбит/с
FTP	64 Кбит/с	64 Кбит/с
E-Mail	64 Кбит/с	64 Кбит/с
Видео	64 Кбит/с	64 Кбит/с

13.5 Приоритеты при управлении пропускной способностью

В следующей таблице представлены приоритеты, применяемые к трафику, проходящему через интерфейс NBG334W.

Табл. 40 Приоритеты при управлении пропускной способностью

УРОВНИ ПРИОРИТЕТОВ: ТРАФИК С БОЛЕЕ ВЫСОКИМ ПРИОРИТЕТОМ ПРОПУСКАЕТСЯ ГОРАЗДО БЫСТРЕЕ, ТОГДА КАК ТРАФИК С БОЛЕЕ НИЗКИМ ПРИОРИТЕТОМ СБРАСЫВАЕТСЯ, ЕСЛИ СЕТЬ ПЕРЕГРУЖЕНА.	
Высокий	Обычно используется для трафика передачи речи или видеоизображений, который очень чувствителен к дрожанию (дрожание – это изменение величины задержки).
Средний	Обычно используется для трафика «excellent effort» или выше по приоритету, чем «best effort» и может включать важный деловой трафик, который допускает некоторую задержку.
Низкий	Обычно используется для второстепенного «низкоприоритетного» трафика, такого как основная масса данных, которая передается, но не влияет на другие приложения и пользователей.

13.6 Предварительно определенные службы управления пропускной способностью

Табл. 41 Настройка управления пропускной способностью: Службы

СЛУЖБА	**ОПИСАНИЕ**
Xbox Live	Это интерактивная игровая служба Microsoft, позволяющая играть в многопользовательские игры Xbox через по сети Интернет через технологию широкополосного доступа. Для службы Xbox Live используется порт 3074.
VoIP (SIP)	Передача речи по Интернет называется Voice over IP или VoIP. Протокол инициирования сеанса связи (Session Initiated Protocol – SIP) является общепризнанным стандартом для обеспечения VoIP. SIP является протоколом уровня приложения (сигнальный протокол), который обеспечивает установку, проведение и завершение голосовых и мультимедиа сеансов связи по Интернет. SIP передается в основном по UDP (Протокол передачи дейтаграмм пользователя), но может передаваться также по TCP с использованием номера порта по умолчанию 5060.
FTP	Протокол передачи файлов позволяет осуществлять быструю передачу файлов, в том числе файлов большого размера, которые невозможно пересылать с помощью электронной почты. Служба FTP использует порт 21.
E-Mail	Электронная почта позволяет передавать сообщения по компьютерной сети конкретному пользователю или группе пользователей. Существует несколько портов, используемых по умолчанию для электронной почты: POP3 – порт 110 IMAP – порт 143 SMTP – порт 25 HTTP – порт 80

Табл. 41 Настройка управления пропускной способностью: Службы (продолжение)

СЛУЖБА	ОПИСАНИЕ
BitTorrent	BitTorrent – это бесплатный инструмент P2P (точка-точка), позволяющий распространять большие объемы программного обеспечения и файлов мультимедиа через порты 6881-6889. BitTorrent требует самостоятельного поиска файла с технологией поиска. Он распространяет файлы путем объединения и обмена, т.е. клиент загружает файл маленькими частями и делится ими с другими узлами, чтобы получить другую половину файла.
MSN Webcam	Служба MSN (Message-switched network – сеть с коммутацией сообщений) позволяет пользователям общаться в интерактивном режиме и отправлять мгновенные сообщения. При использовании клиента MSN и при наличии веб-камеры пользователи могут отправлять изображения и фотографии в реальном режиме времени вместе с сообщениями.
WWW	Всемирная паутина (World Wide Web – WWW) – это система в Интернете, предназначенная для распространения графической и текстовой информации, связанной ссылками, на основе протокола передачи гипертекста (Hyper Text Transfer Protocol – HTTP). HTTP – это протокол типа клиент/сервер, разработанный для WWW. Система Web не является синонимом Интернет; точнее, она является одним из сервисов Интернета. Другими сервисами Интернета являются Интернет-чаты (глобальная система, посредством которой пользователи могут общаться друг с другом в реальном времени) и новостные группы (сетевая служба, рассылающая информацию по определенной теме). К службе Web можно подключиться с помощью браузера.

13.6.1 Службы и номера портов

В следующей таблице приведены наиболее часто используемые службы и номера портов. Дополнительную информацию по номерам портов см. в RFC 1700. Рядом с названием службы располагаются два поля в скобках. В первом поле указывается тип протокола IP (TCP, UDP или ICMP). Во втором – номер порта IP для данной службы. Следует учесть, что тип протокола IP может быть не один. Например, для службы **DNS (UDP/TCP:53)** означает UDP-порт 53 и TCP-порт 53.

Табл. 42 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
AIM/New-ICQ(TCP:5190)	Система пересылки сообщений в сети Интернет, предоставляемая корпорацией AOL, используется службой ICQ как ожидающий порт.
AUTH(TCP:113)	Протокол аутентификации, используемый некоторыми серверами.
BGP(TCP:179)	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT(UDP:68)	Клиент DHCP.
BOOTP_SERVER(UDP:67)	Сервер DHCP.
CU-SEEME(TCP/UDP:7648, 24032)	Популярное решение для проведения видеоконференций от White Pines Software.
DNS(UDP/TCP:53)	Сервер имен доменов – служба, определяющая соответствие web-имен (например, www.zyxel.com) и номеров IP.
FINGER(TCP:79)	Finger – команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.
FTP(TCP:20.21)	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.

Табл. 42 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
H.323(TCP:1720)	Протокол для Net Meeting.
HTTP(TCP:80)	Протокол передачи гипертекста – протокол уровня клиент/сервер для WWW.
HTTPS (TCP:443)	Протокол защищенной передачи текстов, часто используемый в электронной коммерции.
ICQ(UDP:4000)	Популярная система интерактивного общения в Интернет.
IKE(UDP:500)	Алгоритм обмена ключами в Интернет, используется для распределения и управления ключами.
IPSEC_TUNNEL(AH:0)	Эту службу использует протокол туннелирования IPSEC AH (Заголовок аутентификации).
IPSEC_TUNNEL(ESP:0)	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
IRC(TCP/UDP:6667)	Еще одна программа интерактивного общения в Интернет.
MSN Messenger(TCP:1863)	Протокол для передачи сообщений в сетях Microsoft.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отправки пакетов определенным группам узлов.
NEW-ICQ(TCP:5190)	Программа для обмена текстовыми сообщениями между абонентами сети Internet в реальном времени.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система – NFS, распределенная файловая служба клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сети.
NNTP(TCP:119)	Network News Transport Protocol (Сетевой протокол передачи новостей) – система доставки для групп новостей USENET.
PING(ICMP:0)	Packet INternet Groper (Пакетное эхо-тестирование в Интернет) – это протокол, который посылает эхо-запросы ICMP для проверки достижимости удаленного узла.
POP3(TCP:110)	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал управления.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал передачи данных.
RCMD(TCP:512)	Удаленное управление командной строкой.
REAL_AUDIO(TCP:7070)	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в сети в реальном времени.
REXEC(TCP:514)	Daemon-служба удаленного выполнения команд.
RLOGIN(TCP:513)	Удаленная регистрация.
RTELNET(TCP:107)	Удаленный доступ через Telnet.
RTSP(TCP/UDP:554)	Протокол (Real Time Streaming – Протокол воспроизведения в реальном времени) – это удаленное управление для мультимедиа в Интернете.
SFTP(TCP:115)	Простой протокол передачи файлов.

Табл. 42 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
SMTP(TCP:25)	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SNMP(TCP/UDP:161)	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS(TCP/UDP:162)	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language (Язык структурированных запросов) представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, системы средней производительности, системы UNIX и сетевые серверы.
SSH(TCP/UDP:22)	Программа безопасной удаленной регистрации.
STRM WORKS(UDP:1558)	Протокол передачи потоков Stream Works.
SYSLOG(UDP:514)	Системный журнал – позволяет отправлять журналы системы серверу UNIX.
TACACS(UDP:49)	Login Host Protocol (Протокол регистрации узла), используется для TACACS (Terminal Access Controller Access Control System – Система управления доступом на основе контроллера доступа к терминалу).
TELNET(TCP:23)	Telnet – протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах.
TFTP(UDP:69)	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE(TCP:7000)	Еще одна программа для видеоконференций.

13.7 Стандартные классы и приоритеты управления пропускной способностью

Если при включении управления полосой пропускания не настроить правило для критичного трафика, например, VoIP, то возможна задержка этого голосового трафика из-за недостатка пропускной способности. При включении автоматической классификации трафика на NBG334W, трафику, который не подпадает ни под одно заданное пользователем правило, предоставляется стандартный класс и приоритет управления пропускной способностью. Классификация трафика выполняется на основе его типа. Трафик, передаваемый в реальном масштабе времени всегда имеет повышенный приоритет по сравнению с трафиком других типов.

В следующей таблице приведены приоритеты для трех стандартных классов (**AutoClass_H**, **AutoClass_M** и **Default Class**) и определяемых пользователями правил. 6 означает самый высокий приоритет.

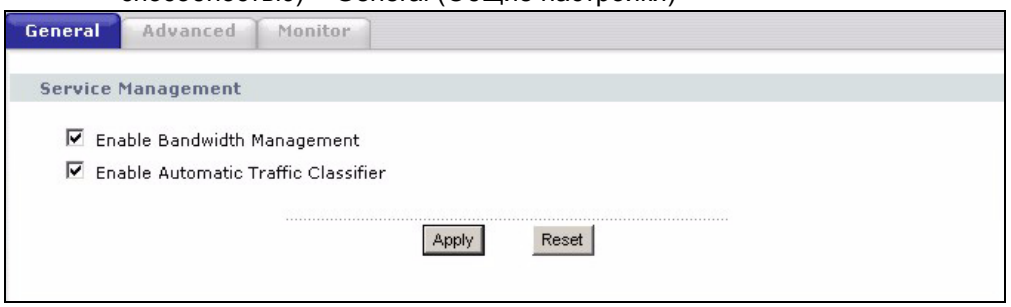
Табл. 43 Приоритет управления пропускной способностью для стандартных классов

ТИП КЛАССА	ПРИОРИТЕТ
User-defined with high priority (Определяемый пользователем с высоким приоритетом)	6
AutoClass_H	5
User-defined with high priority (Определяемый пользователем со средним приоритетом)	4
AutoClass_M	3
User-defined with high priority (Определяемый пользователем с низким приоритетом)	2
Default Class (Стандартный класс)	1

13.8 Общая настройка управления пропускной способностью

Щелкните **Management (Управление) > Bandwidth MGMT (Управление пропускной способностью)**, чтобы открыть окно **общей (General)** настройки пропускной способности.

Рис. 55 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > General (Общие настройки)



В следующей таблице даны описания полей этого окна.

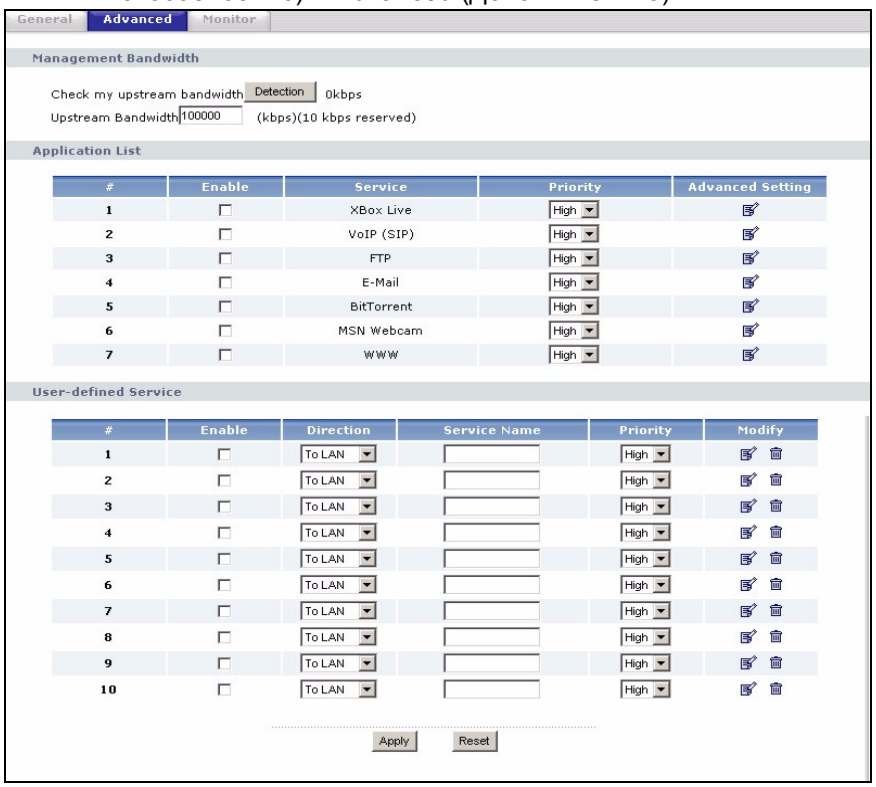
Табл. 44 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > General (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
Enable Bandwidth Management (Включить управление пропускной способностью)	Установите этот флажок, чтобы включить управление пропускной способностью на интернет-центре NBG334W. Включите управление пропускной способностью, чтобы назначить трафику, который соответствует правилу, приоритет над трафиком, который не соответствует правилу управления пропускной способностью. Включение правила управления пропускной способностью позволяет также контролировать максимальную или минимальную величину пропускной способности, которая может использоваться трафиком, соответствующим правилу управления пропускной способностью.
Enable Automatic Traffic Classifier (Включить автоматическую классификацию трафика)	Это поле используется только в том случае, если установлен флажок в поле **Enable Bandwidth Management (Включить управление пропускной способностью)**. Установите этот флажок, чтобы включить управление пропускной способностью на интернет-центре NBG334W на основе стандартных классов. При этом пакеты, передаваемые в реальном масштабе времени, например, трафик VoIP, будут передаваться с повышенным приоритетом.
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения произведенных настроек.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

13.9 Расширенная настройка управления пропускной способностью

Щелкните **Management (Управление)** > **Bandwidth MGMT (Управление пропускной способностью)** > **Advanced (Дополнительно)**, чтобы открыть окно **расширенной (Advanced)** настройки пропускной способности.

Рис. 56 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced (Дополнительно)



В следующей таблице даны описания полей этого окна.

Табл. 45 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced (Дополнительно)

ПОЛЕ	ОПИСАНИЕ
Check my upstream bandwidth (Проверить пропускную способность восходящего потока)	Нажмите кнопку **Detection (Обнаружение)**, чтобы проверить ширину полосы пропускания восходящего потока.
Upstream Bandwidth (kbps) (Восходящий поток (в Кбит/с))	Введите ширину полосы пропускания трафика в Кбит/с (от 2 до 100 000). Рекомендуется указывать 20-20 000 Кбит/с. Также не рекомендуется указывать скорость, большую, чем скорость пропускания устройства, подключенного к порту WAN. Например,если скорость восходящего потока устройства, подключенного к порту WAN, составляет 1000 Кбит/с, установите именно эту скорость (или менее).
Application List (Список приложений)	Позволяет указать долю пропускной способности для каждой из определенных служб.
#	Это номер конкретного правила управления пропускной способностью.

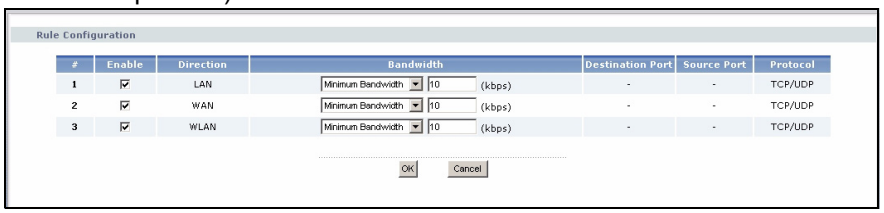
Табл. 45 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced (Дополнительно) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable (Включить)	Установите в этом поле флажок, чтобы NBG334W применял данное правило управления пропускной способностью.
Service (Служба)	В этом поле отображается название службы.
Priority (Приоритет)	Выберите приоритет из раскрывающегося списка. Вариантами являются: **High (Высокий)**, **Mid (Средний)** или **Low (Низкий)**.
Advanced Setting (Дополнительная настройка)	Щелкните значок **Edit (Правка)**, чтобы открыть окно **Rule Configuration (Настройка правила)**, в котором можно изменить правило.
User-defined Service (Служба, определенная пользователем)	В данной таблице можно указать долю пропускной способности для конкретных приложений и подсетей.
#	Это номер конкретного правила управления пропускной способностью.
Enable (Включить)	Установите в этом поле флажок, чтобы NBG334W применял данное правило управления пропускной способностью.
Direction (Направление)	Выберите вариант **To LAN (В локальную сеть)**, чтобы разрешить интернет-центра NBG334W управлять трафиком, поступающим в локальную сеть. Выберите вариант **To WAN (В глобальную сеть)**, чтобы разрешить интернет-центру NBG334W управлять трафиком, отправляемым в глобальную сеть. Выберите вариант **To WLAN (В беспроводную локальную сеть)**, чтобы разрешить интернет-центру NBG334W управлять трафиком, поступающим в беспроводную локальную сеть.
Service Name (Название службы)	Введите описательное имя длиной не более 19 алфавитно-цифровых символов, включая пробелы.
Priority (Приоритет)	Выберите приоритет из раскрывающегося списка. Вариантами являются: **High (Высокий)**, **Mid (Средний)** или **Low (Низкий)**.
Modify (Изменить)	Щелкните значок **Edit (Правка)**, чтобы открыть окно **Rule Configuration (Настройка правила)**. В этом окне можно создать новое или изменить существующее правило. Более подробную информацию см. в Разд. 13.9.2 на с. 136. Для удаления правила щелкните значок **Remove (Удалить)**.
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения произведенных настроек.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

13.9.1 Настройка правила для стандартной службы

Для редактирования правила управления пропускной способностью для стандартной службы интернет-центра NBG334W щелкните значок **Edit (Правка)** в таблице **Application List (Список приложений)** окна **Advanced (Дополнительно)**. Появится следующее окно.

Рис. 57 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced: Rule Configuration (Дополнительно: настройка правила)



В следующей таблице даны описания полей этого окна.

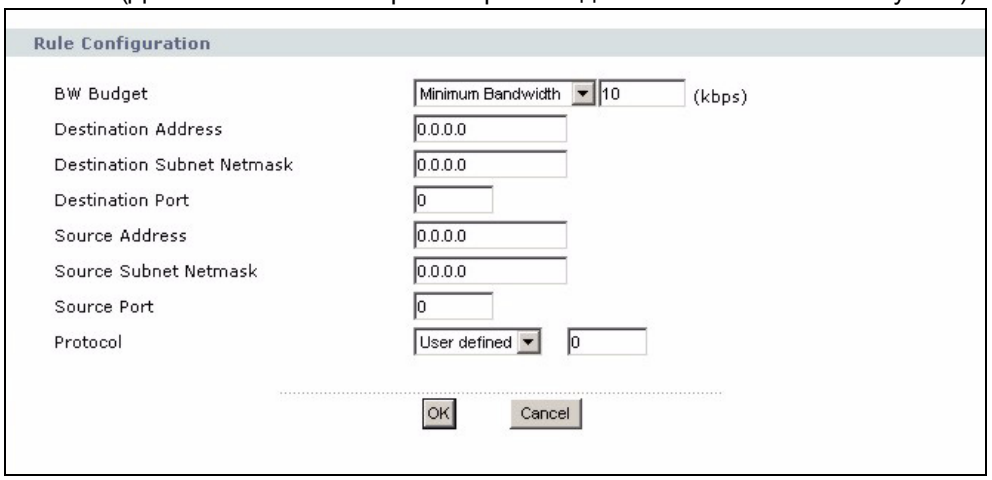
Табл. 46 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced: Application Rule Configuration (Дополнительно: настройка правила приложения)

ПОЛЕ	ОПИСАНИЕ
#	Это номер конкретного правила управления пропускной способностью.
Enable (Включить)	Для включения управления пропускной способностью того или иного интерфейса поставьте флажок напротив его названия.
Direction (Направление)	Эти поля «только для чтения» обозначают физические интерфейсы. Управление пропускной способностью применяется ко всему трафику, выходящему через интерфейс маршрутизатора, независимо от источника этого трафика. Перенаправление трафика и псевдонимы IP могут вызвать трафик между локальными сетями, который проходит через NBG334W, и следовательно, регулируется системой управления пропускной способностью.
Bandwidth (Пропускная способность)	Выберите вариант **Maximum Bandwidth (Максимальная пропускная способность)** или **Minimum Bandwidth (Минимальная пропускная способность)** и укажите, соответственно, максимальную или минимальную пропускную способность в Кбит/с, разрешенную правилом.
Destination Port (Порт получателя)	Это номер порта получателя. Информация о распространенных службах и номерах портов: см. Табл. 42 на с. 128.
Source Port (Порт источника)	Это номер порта отправителя. Информация о распространенных службах и номерах портов: см. Табл. 42 на с. 128.
Protocol (Протокол)	Это протокол (**TCP** или **UDP**), используемый службой.
OK	Нажмите кнопку **OK** для сохранения произведенных настроек.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отмена)**, чтобы выйти из этого окна без сохранения изменений.

13.9.2 Настройка правила для пользовательской службы

Чтобы, в дополнение к стандартным службам, создать правило управления пропускной способностью для других приложений и подсетей, щелкните значок **Edit (Правка)** в таблице **User-defined Service (Пользовательская служба)** окна **Advanced (Дополнительно)**. Появится следующее окно.

Рис. 58 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced: User-defined Service Rule Configuration (Дополнительно: настройка правила для пользовательской службы)



В следующей таблице даны описания полей этого окна.

Табл. 47 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced: User-defined Service Rule Configuration (Дополнительно: настройка правила для пользовательской службы)

ПОЛЕ	ОПИСАНИЕ
BW Budget (Бюджет пропускной способности)	Выберите вариант **Maximum Bandwidth (Максимальная пропускная способность)** или **Minimum Bandwidth (Минимальная пропускная способность)** и укажите, соответственно, максимальную или минимальную пропускную способность в Кбит/с, разрешенную правилом.
Destination Address (Адрес получателя)	Введите IP-адрес получателя в десятичном виде с разделительными точками.
Destination Subnet Netmask (Маска подсети получателя)	Введите маску подсети получателя. Это поле будет недоступно, если не установлен **Destination Address (Адрес получателя)**. Для получения дополнительной информации о подсетях IP см. приложения.
Destination Port (Порт получателя)	Введите номер порта получателя. Информация о распространенных службах и номерах портов: см. Табл. 42 на с. 128.
Source Address (Адрес источника)	Введите IP-адрес источника в десятичном виде с разделительными точками.
Destination Subnet Netmask (Маска подсети источника)	Введите маску подсети получателя. Это поле будет недоступно, если не установлен **Source Address (Адрес источника)**. Для получения дополнительной информации о подсетях IP см. приложения.
Source Port (Порт источника)	Введите номер порта отправителя. Информация о распространенных службах и номерах портов: см. Табл. 42 на с. 128.

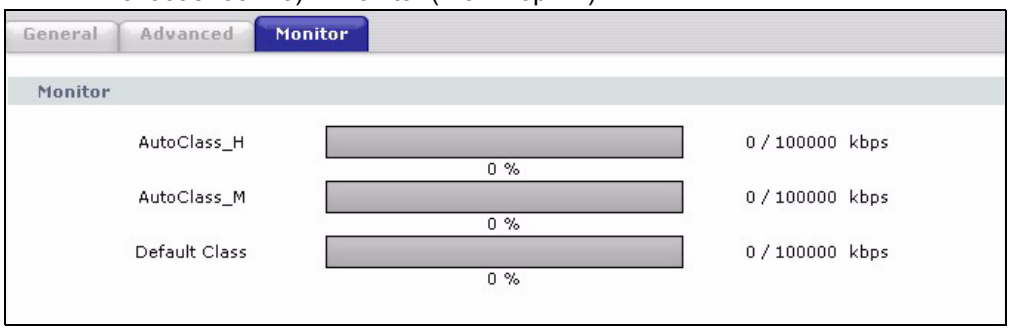
Табл. 47 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Advanced: User-defined Service Rule Configuration (Дополнительно: настройка правила для пользовательской службы)

ПОЛЕ	ОПИСАНИЕ
Protocol (Протокол)	Выберите протокол (**TCP** или **UDP**) или установите **User defined (Определяется пользователем)** и введите номер протокола (тип службы).
OK	Нажмите кнопку **OK** для сохранения произведенных настроек.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отмена)**, чтобы выйти из этого окна без сохранения изменений.

13.10 Мониторинг управления пропускной способностью

Щелкните **Management (Управление)** > **Bandwidth MGMT (Управление пропускной способностью)** > **Monitor (Мониторинг)**, чтобы открыть окно **Monitor (Мониторинг)**. Обратите внимание на использование пропускной способности правилами работы с WAN. Здесь также отображается использование пропускной способности относительно ее бюджета для каждого правила. Серая часть индикатора показывает неиспользуемую пропускную способность в процентах, а оранжевый цвет показывает используемую пропускную способность.

Рис. 59 Management (Управление) > Bandwidth MGMT (Управление пропускной способностью) > Monitor (Мониторинг)



14

Удаленное управление

В этой главе описываются окна удаленного управления устройством.

14.1 Удаленное управление – общая информация

При помощи удаленного управления можно определить службы/протоколы для доступа к NBG334W, интерфейс управления, а также компьютеры, с которых можно выполнять управление интернет-центром.

При установке параметров конфигурации удаленного управления, предназначенного для реализации функций управления через глобальную вычислительную сеть (WAN), необходимо также настроить правило межсетевого экрана разрешения доступа к устройству. Более подробно о настройках правил межсетевого экрана см. главы, посвященные межсетевому экрану.

Возможны следующие режимы удаленного управления NBG334W:

- только через глобальную сеть (Интернет)
- только через локальную сеть
- отовсюду (через локальную и глобальную сеть)
- отключено

При выборе **WAN (Глобальная сеть)** или **LAN & WAN (Локальная и глобальная сеть)** необходимо также настроить правило межсетевого экрана для разрешения доступа к устройству.

Чтобы отключить удаленное управление конкретной службой, выберите **Disable (Отключить)** в соответствующем поле **Server Access (Доступ к серверу)**.

Одновременно допускается проведение только одного сеанса удаленного управления. NBG334W автоматически завершает сеанс удаленного управления с более низким приоритетом, если запускается другой сеанс удаленного управления, имеющий более высокий приоритет. Для сеансов удаленного управления существуют следующие приоритеты:

1. Telnet
2. HTTP

14.1.1 Ограничения на удаленное управление

Удаленное управление через локальную или глобальную сеть не будет работать, если:

1. Эта служба отключена в окне настройки удаленного управления.
2. IP-адрес, установленный в поле **Secured Client IP (IP-адрес доверенного клиента)**, не совпадает с IP-адресом клиента. В случае несовпадения NBG334W немедленно завершает сеанс связи.
3. Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. Одновременно допускается проведение только одного сеанса удаленного управления.
4. Существует правило межсетевого экрана, блокирующее удаленное управление.

14.1.2 Удаленное управление и NAT

Если функция трансляции сетевых адресов (NAT) включена, то:

- При управлении из глобальной сети необходимо использовать IP-адрес NBG334W в глобальной сети;
- При управлении из локальной сети необходимо использовать IP-адрес NBG334W в локальной сети.

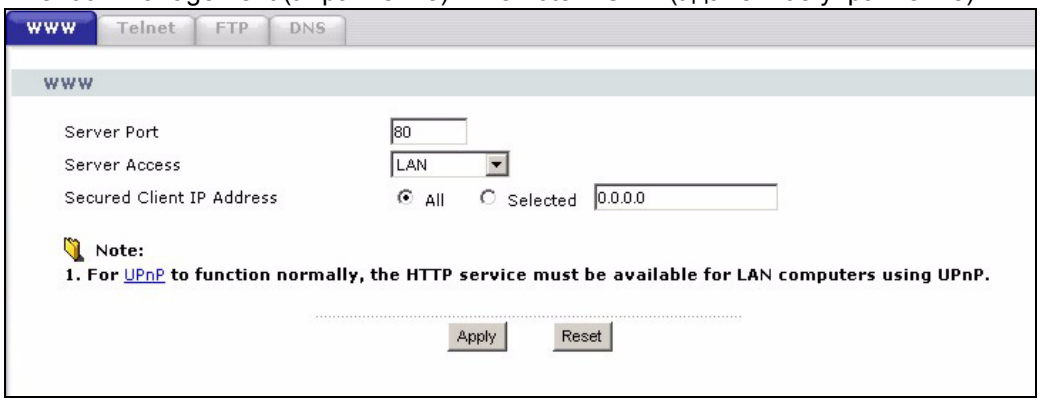
14.1.3 Время простоя системы

Максимальное время простоя системы во время сеанса управления по умолчанию установлено на 5 минут (300 секунд). Интернет-центр NBG334W автоматически завершает сеанс управления при простое, продолжающемся более этого периода. Сеанс управления не разрывается, если в окне статистики проводится опрос системы. Время простоя можно изменить в окне **System (Система)**.

14.2 Окно WWW

Для изменения параметров подключения NBG334W к глобальной сети щелкните **Management (Управление)** > **Remote MGMT (Удаленное управление)** для отображения окна **WWW**.

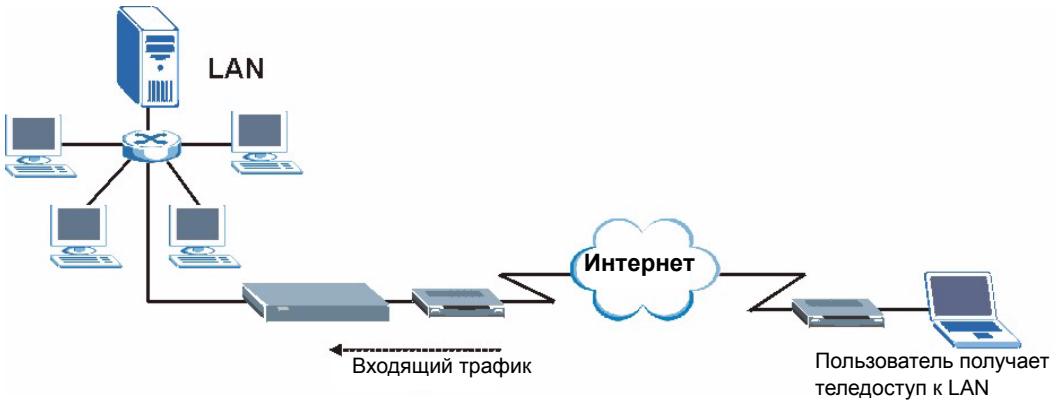
Рис. 60 Management (Управление) > Remote MGMT (Удаленное управление) > WWW



14.3 Управление с помощью Telnet

Можно настроить удаленный доступ к NBG334W через Telnet, как показано ниже. Администратор с компьютера в удаленной сети подключается к NBG334W с помощью Telnet.

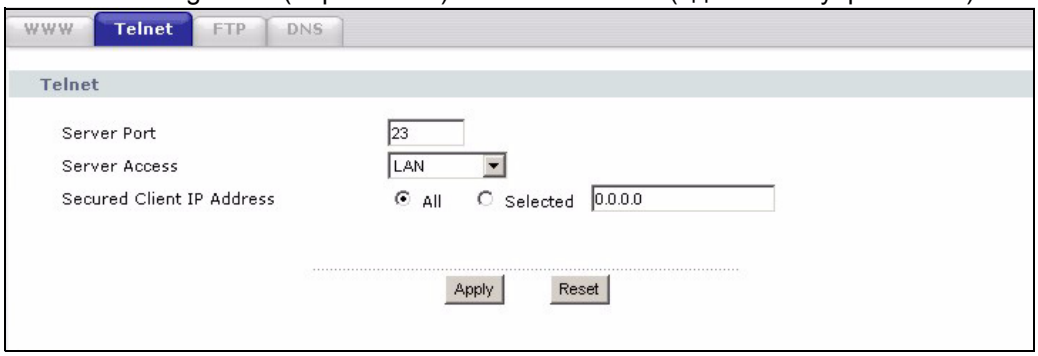
Рис. 61 Настройка Telnet в сети TCP/IP



14.4 Окно Telnet

Для изменения настроек **Telnet** в NBG334W щелкните **Management (Управление)** > **Remote MGMT (Удаленное управление) > Telnet**. Появится следующее окно.

Рис. 62 Management (Управление) > Remote MGMT (Удаленное управление) > Telnet



В следующей таблице даны описания полей этого окна.

Табл. 48 Management (Управление) > Remote MGMT (Удаленное управление) > Telnet

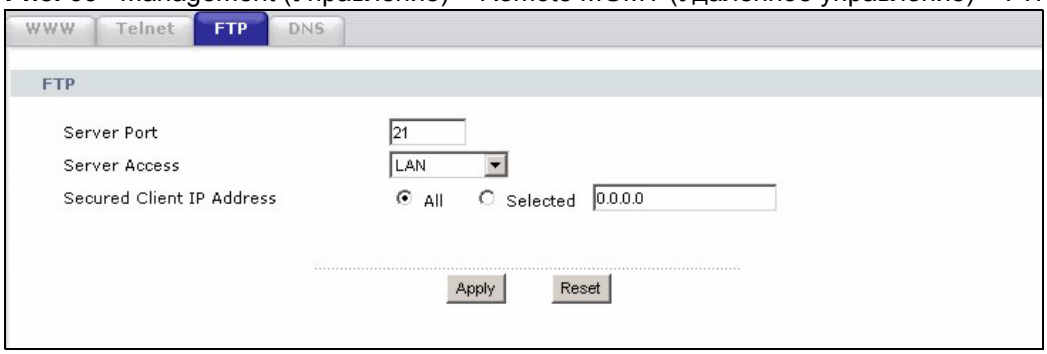
ПОЛЕ	ОПИСАНИЕ
Server Port (Порт сервера)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Server Access (Доступ к серверу)	Выберите интерфейсы, через которые компьютер сможет получить доступ к NBG334W при использовании этой службы.
Secured Client IP Address (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к NBG334W при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к NBG334W при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к NBG334W только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

14.5 Окно FTP

С помощью FTP можно выполнять загрузку и выгрузку микропрограммы NBG334W, а также файлов конфигурации, подробнее см. главу о микропрограмме и сопровождении файлов конфигурации. Для использования данной функции на компьютере должен быть установлен FTP-клиент.

Для изменения настроек FTP в NBG334W щелкните **Management (Управление)** > **Remote MGMT (Удаленное управление) > FTP**. При этом откроется следующее окно.

Рис. 63 Management (Управление) > Remote MGMT (Удаленное управление) > FTP



В следующей таблице даны описания полей этого окна.

Табл. 49 Management (Управление) > Remote MGMT (Удаленное управление) > FTP

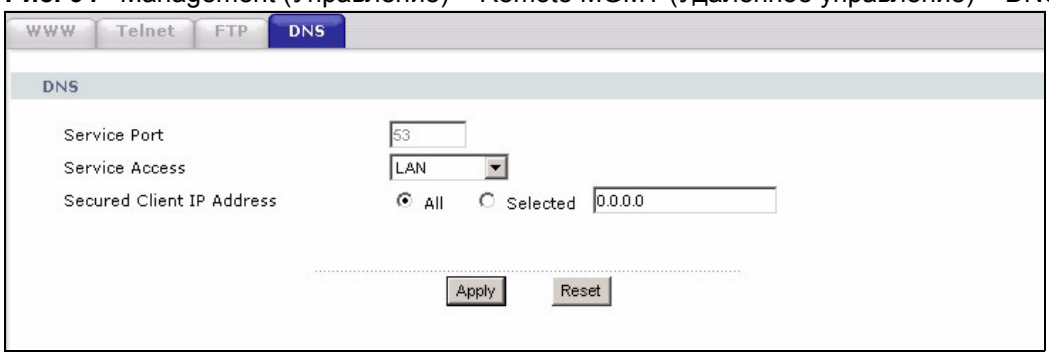
ПОЛЕ	ОПИСАНИЕ
Server Port (Порт сервера)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Server Access (Доступ к серверу)	Выберите интерфейсы, через которые компьютер сможет получить доступ к NBG334W при использовании этой службы.
Secured Client IP Address (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к NBG334W при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к NBG334W при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к NBG334W только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

14.6 Окно DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот.

Для изменения настроек DNS в NBG334W щелкните **Management (Управление)** > **Remote MGMT (Удаленное управление) > DNS**. При этом откроется следующее окно.

Рис. 64 Management (Управление) > Remote MGMT (Удаленное управление) > DNS



В следующей таблице даны описания полей этого окна.

Табл. 50 Management (Управление) > Remote MGMT (Удаленное управление) > DNS

ПОЛЕ	ОПИСАНИЕ
Server Port (Порт сервера)	Номер служебного порта DNS – 53, и его нельзя изменить здесь.
Server Access (Доступ к серверу)	Выберите интерфейсы, через которые компьютер сможет посылать NBG334W запросы DNS.
Secured Client IP Address (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается посылать NBG334W запросы DNS. Выберите **All (Все)**, чтобы разрешить любому компьютеру посылать NBG334W запросы DNS. Выберите **Selected (Выбранный)**, чтобы разрешить NBG334W посылать запросы DNS только компьютеру с указанным IP-адресом.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

15

Универсальная функция Plug and Play (UPnP)

В данной главе представлена информация о функции UPnP в Web-конфигураторе.

15.1 Описание универсальной функции Plug and Play

Универсальная функция Plug and Play (UPnP) – это распространенный открытый сетевой стандарт, использующий TCP/IP для обеспечения взаимодействия между устройствами в одноранговой сети. Устройство UPnP может динамически подключаться к сети, получать IP-адрес, предоставлять свои ресурсы и собирать информацию о других устройствах сети. Кроме того, устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

Инструкции по настройке см. Разд. 15.3 на с. 146.

15.1.1 Как узнать, используется ли UPnP?

Оборудование UPnP идентифицируется значком в папке **Network Connections (Сетевые подключения)** (Windows XP). Каждое совместимое с UPnP устройство, установленное в сети, появляется в виде отдельного значка. Выбор значка устройства UPnP позволяет получить доступ к информации и свойствам данного устройства.

15.1.2 NAT Transversal

Функция NAT Traversal с поддержкой UPnP автоматизирует процесс работы приложения через NAT. Сетевые устройства UPnP могут автоматически настраивать сетевую адресацию, объявлять о своем присутствии в сети другим устройствам UPnP и производить обмен простыми сообщениями о программных продуктах и службах. Функция NAT Traversal позволяет следующее:

- Динамическое отображение портов
- Распознавание общедоступных IP-адресов
- Назначение времени аренды для отображений

Windows Messenger является примером приложения, которое поддерживает NAT traversal и UPnP.

Для получения более подробной информации о NAT см. главу по трансляции сетевых адресов.

15.1.3 Предупреждения по использованию UPnP

Автоматический характер приложений NAT traversal при установке их собственных служб и открывании портов межсетевого экрана может привести к проблемам в отношении безопасности сети. В некоторых сетевых окружениях пользователи могут получить доступ к сетевой информации и конфигурации, а также к ее изменению.

Когда устройство UPnP подключается к сети, оно объявляет о своем присутствии с помощью многоадресной рассылки сообщения. Из соображений безопасности NBG334W разрешает многоадресную рассылку сообщений только по локальной сети.

Все устройства с включенной функцией UPnP могут свободно взаимодействовать друг с другом без дополнительной настройки. Отключите функцию UPnP, если ее не предполагается использовать.

15.2 UPnP и ZyXEL

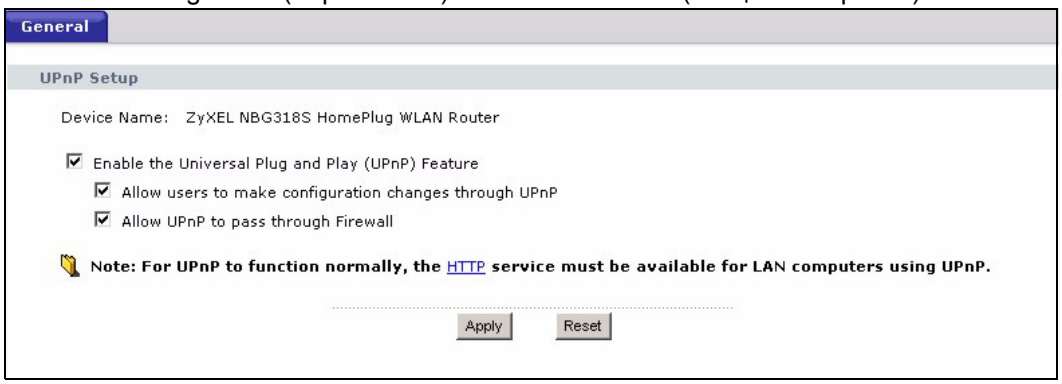
Корпорация ZyXEL получила сертификат от организации Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Реализация UPnP корпорации ZyXEL поддерживает IGD 1.0 (Internet Gateway Device – Устройство Интернет-шлюза).

Примеры установки и использования UPnP см. в следующих разделах.

15.3 Окно UPnP

Щелкните **Management (Управление)** > **UPnP** для отображения окна, показанного ниже.

Рис. 65 Management (Управление) > UPnP > General (Общие настройки)



В следующей таблице даны описания полей этого окна.

Табл. 51 Management (Управление) > UPnP > General (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
Enable the Universal Plug and Play (UPnP) Feature (Включить функцию UPnP)	Установите флажок в этом окне для включения UPnP. Помните, что любой может с помощью приложения UPnP открыть окно регистрации Web-конфигуратора без ввода IP-адреса интернет-центра NBG334W (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Allow users to make configuration changes through UPnP (Разрешить пользователям вносить изменения в конфигурацию через UPnP)	Установите здесь флажок, чтобы разрешить приложениям с включенной функцией UPnP автоматически выполнять настройку NBG334W для того, чтобы они могли взаимодействовать через NBG334W. Например, с помощью обхода NAT приложения UPnP автоматически резервируют порт переадресации NAT, чтобы взаимодействовать с другим устройством UPnP. Это устраняет необходимость ручной настройки переадресации портов для приложений UPnP.
Allow UPnP to pass through Firewall (Разрешить прохождение UPnP через межсетевой экран)	Поставьте галочку, если нужно разрешить прохождение трафика от приложений, использующих универсальные средства Plug&Play (UPnP) через межсетевой экран. Снимите флажок, если межсетевой экран должен блокировать все пакеты приложений на базе UPnP (например, пакеты MSN).
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения настроек NBG334W.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

15.4 Пример установки UPnP в Windows

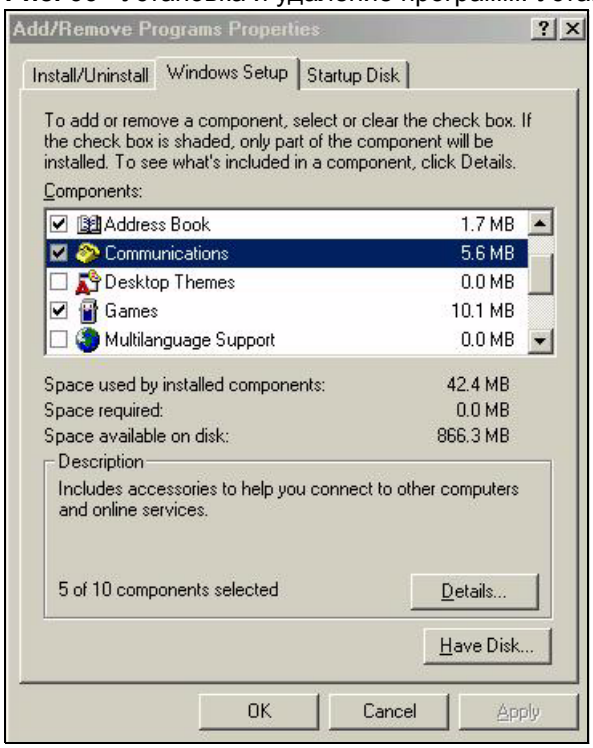
В данном разделе описывается установка UPnP в Windows Me и Windows XP.

15.4.0.1 Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

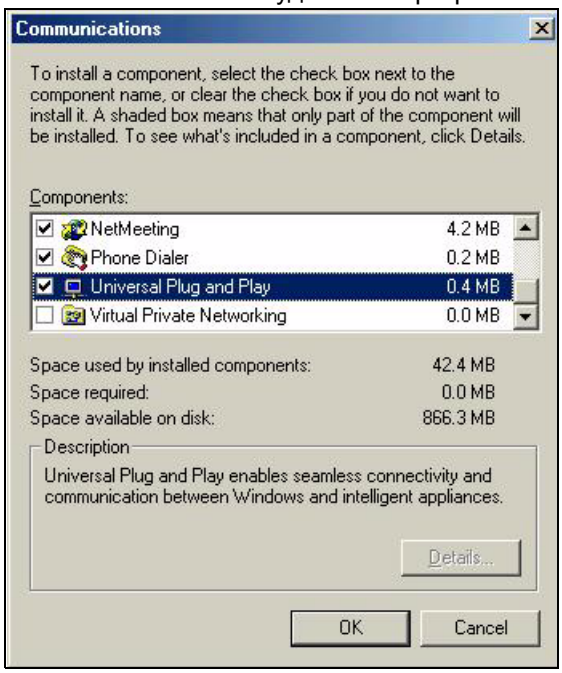
1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните пункт **Add/Remove Programs (Установка и удаление программ)**.
2. Выберите закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Нажмите **Details (Состав)**.

Рис. 66 Установка и удаление программ: Установка Windows: Связь



3 В окне **Communications (Связь)** в поле **Components (Компоненты)** установите флажок **Universal Plug and Play**.

Рис. 67 Установка и удаление программ: Установка Windows: Связь: Компоненты



4 Нажмите **OK** для возврата в окно **Add/Remove Programs Properties (Свойства: Установка и удаление программ)** и нажмите **Next (Далее)**.

5 При появлении запроса перезагрузите компьютер.

Установка UPnP в Windows XP

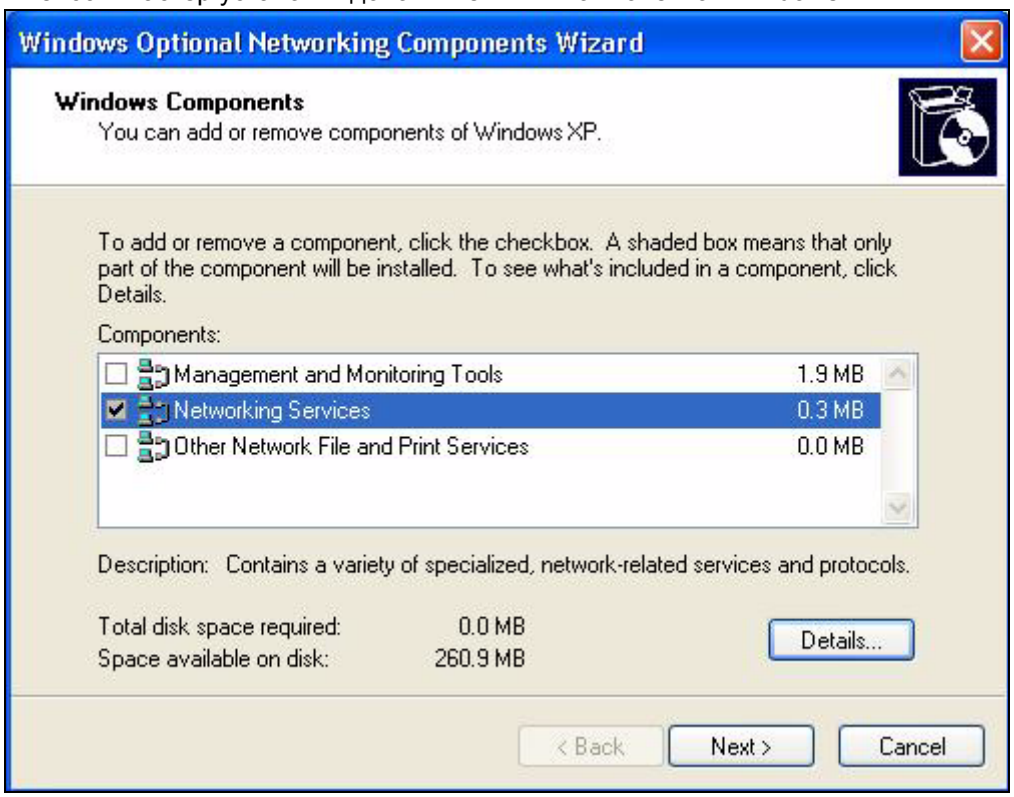
Выполните следующие действия для установки UPnP в Windows XP.

1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**.
2. Дважды щелкните значок **Network Connections (Сетевые подключения)**.
3. В окне **Network Connections (Сетевые подключения)** нажмите кнопку **Advanced (Дополнительно)** в главном меню и выберите **Optional Networking Components… (Дополнительные сетевые компоненты...)**.

Рис. 68 Сетевые подключения

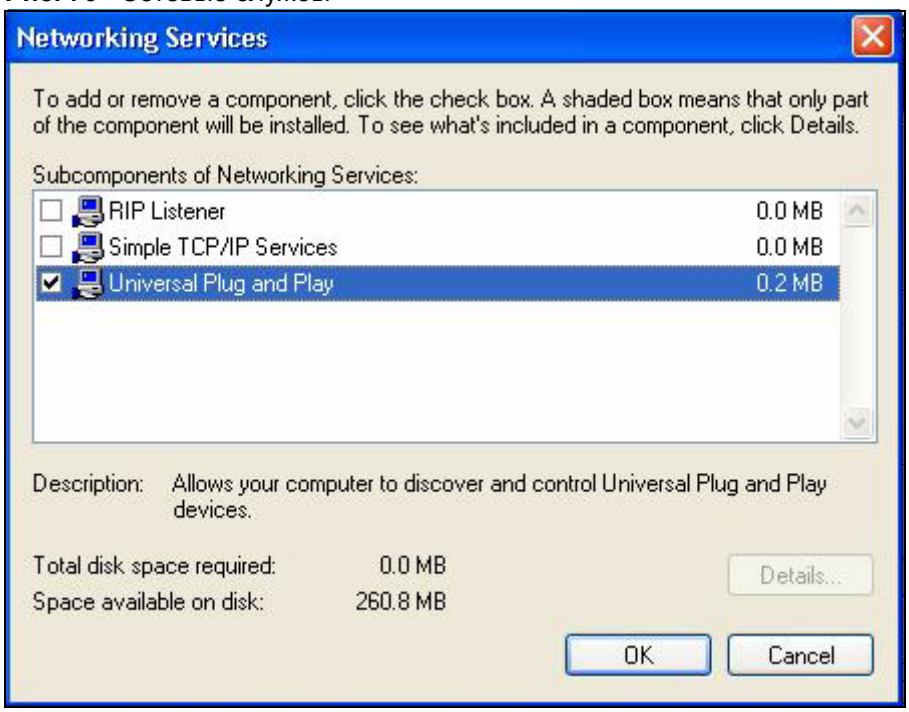
4. Появляется окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите **Networking Services (Сетевые службы)** в поле **Components (Компоненты)** и нажмите **Details (Состав)**.

Рис. 69 Мастер установки дополнительных компонентов Windows



5 В окне **Networking Services (Сетевые службы)** поставьте флажок **Universal Plug and Play**.

Рис. 70 Сетевые службы



6 Нажмите **OK** для возврата в окно **Windows Optional Networking Component Wizard (Мастер установки дополнительных сетевых компонентов Windows)** и нажмите **Next (Далее)**.

15.4.0.2 Пример использования UPnP в Windows XP

В этом разделе описывается использование функции UPnP в Windows XP. Функция UPnP уже должна быть установлена в Windows XP и включена в интернет-центре NBG334W.

Убедитесь, что компьютер подключен к порту LAN интернет-центра NBG334W. Включите компьютер и NBG334W.

Автоматическое обнаружение сетевого устройства UPnP

1 Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните значок **Network Connections (Сетевые подключения)**. В разделе **Internet Gateway (Шлюз в Интернет)** отображается значок.

2 Щелкните правой кнопкой мыши на этом значке и выберите **Properties (Свойства)**.

Рис. 71 Сетевые подключения

3 В окне **Internet Connection Properties (Свойства подключения к Интернет)**, нажмите **Settings (Настройки)** для просмотра автоматически созданных правил отображения портов.

Рис. 72 Свойства подключения к Интернет

4 Вы можете редактировать или удалять правила отображения портов, или щелкнуть по кнопке **Add (Добавить)**, чтобы вручную добавить правило отображения портов.

Рис. 73 Свойства подключения к Интернет: Дополнительные настройки

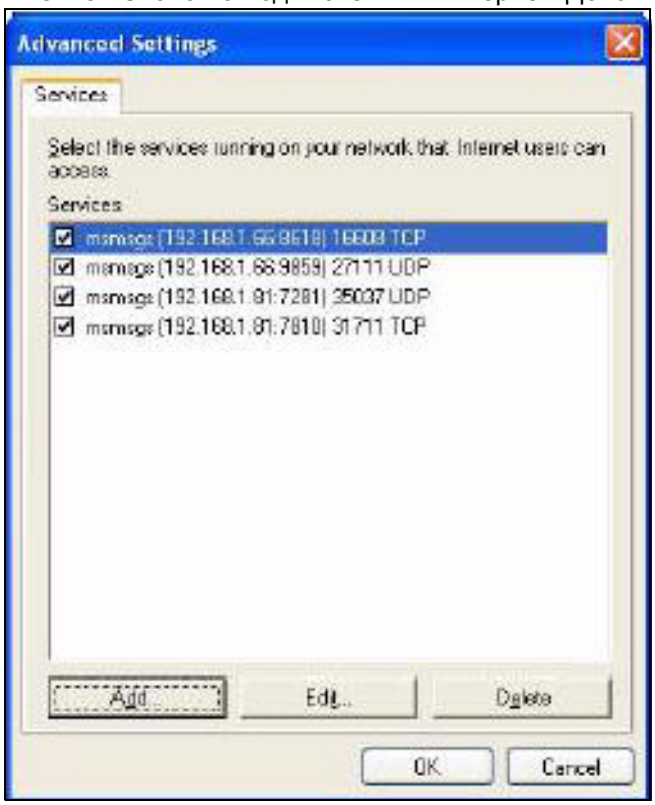
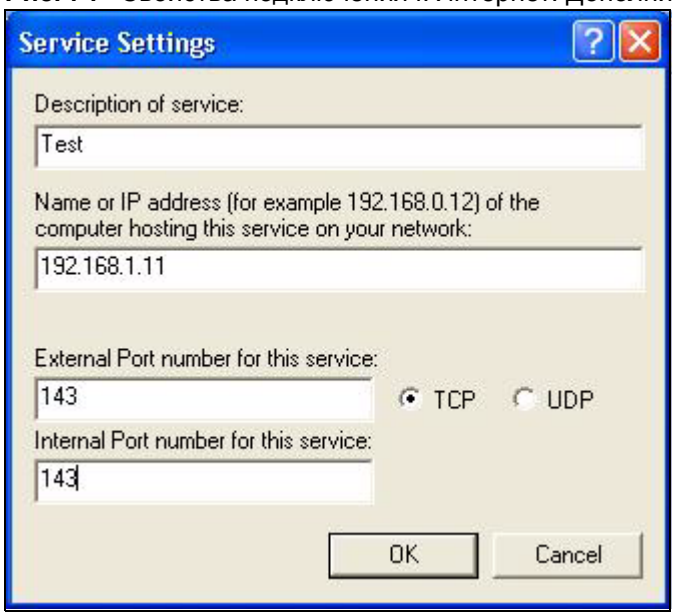


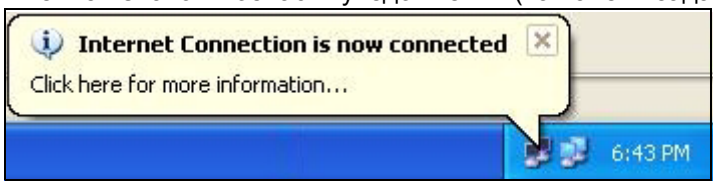
Рис. 74 Свойства подключения к Интернет: Дополнительные настройки: Добавить



5 При отключении устройства UPnP от компьютера все правила отображения портов автоматически удаляются.

6 Выберите **Show icon in notification area when connected (При подключении вывести значок в области уведомлений)** и нажмите **OK**. На панели задач появится значок.

Рис. 75 Значок в области уведомлений (на панели задач)



7 Дважды щелкните значок для отображения текущего состояния подключения к Интернету.

Рис. 76 Состояние подключения к Интернет

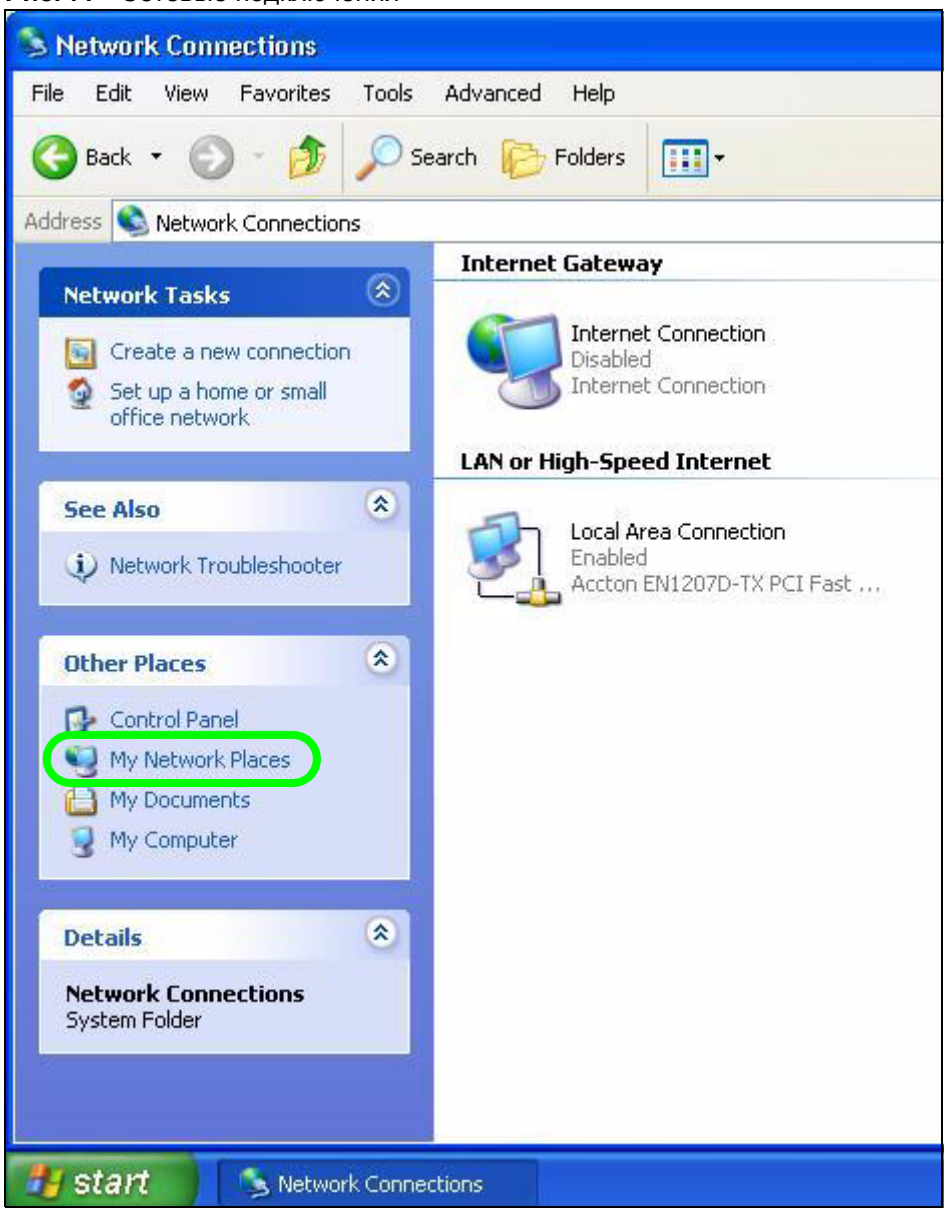
Простой доступ к Web-конфигуратору

С помощью UPnP вы можете получить доступ к программе настройки NBG334W на основе Web технологии без предварительного выяснения IP-адреса NBG334W. Это может оказаться полезным, если вы не знаете IP-адрес NBG334W.

Выполните следующие действия для доступа к Web-конфигуратору.

1 Нажмите кнопку **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**.
2 Дважды щелкните значок **Network Connections (Сетевые подключения)**.
3 Выберите **My Network Places (Сетевое окружение)** в разделе **Other Places (Другие места)**.

Рис. 77 Сетевые подключения



4 В разделе **Local Network (Локальная сеть)** для каждого UPnP-совместимого устройства отображается значок с описанием.

5 Щелкните правой кнопкой мыши по значку NBG334W и выберите **Invoke (Запустить)**. Появится окно регистрации Web-конфигуратора.

Рис. 78 Сетевые подключения: Сетевое окружение

6 Щелкните правой кнопкой мыши по значку NBG334W и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией об интернет-центре NBG334W.

Рис. 79 Пример – Сетевые подключения: Сетевое окружение: Свойства

Часть V
Обслуживание, поиск и устранение неисправностей

Система (159)
Регистрационные журналы (165)
Программные средства (183)
Поиск и устранение неисправностей (189)

16

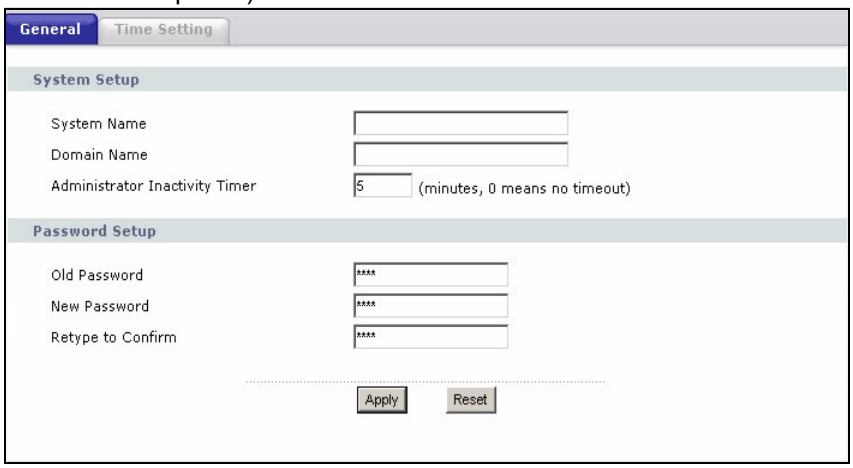
Система

В данной главе описываются окна **Системы**.

16.1 Окно общей настройки системы

Щелкните пункт **Maintenance (Сопровождение)** > **System (Система)**. Появится следующее окно.

Рис. 80 Maintenance (Сопровождение) > System (Система) > General (Общие настройки)



В следующей таблице даны описания полей этого окна.

Табл. 52 Maintenance (Сопровождение) > System (Система) > General (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
System Name (Системное имя)	Системное имя – это уникальный идентификатор интернет-центра NBG334W в сети Ethernet. Рекомендуется в качестве системного имени использовать имя Вашего компьютера. Имя может включать до 30 буквенно-цифровых символов. Пробелы не допускаются, но допускаются тире «-» и знак подчеркивания «_».
Domain Name (Доменное имя)	Введите в это поле доменное имя (если оно известно). Если это поле оставлено пустым, Интернет-провайдер может назначить доменное имя с помощью DHCP. Введенное доменное имя обладает более высоким приоритетом, чем доменное имя, назначенное Интернет-провайдером.

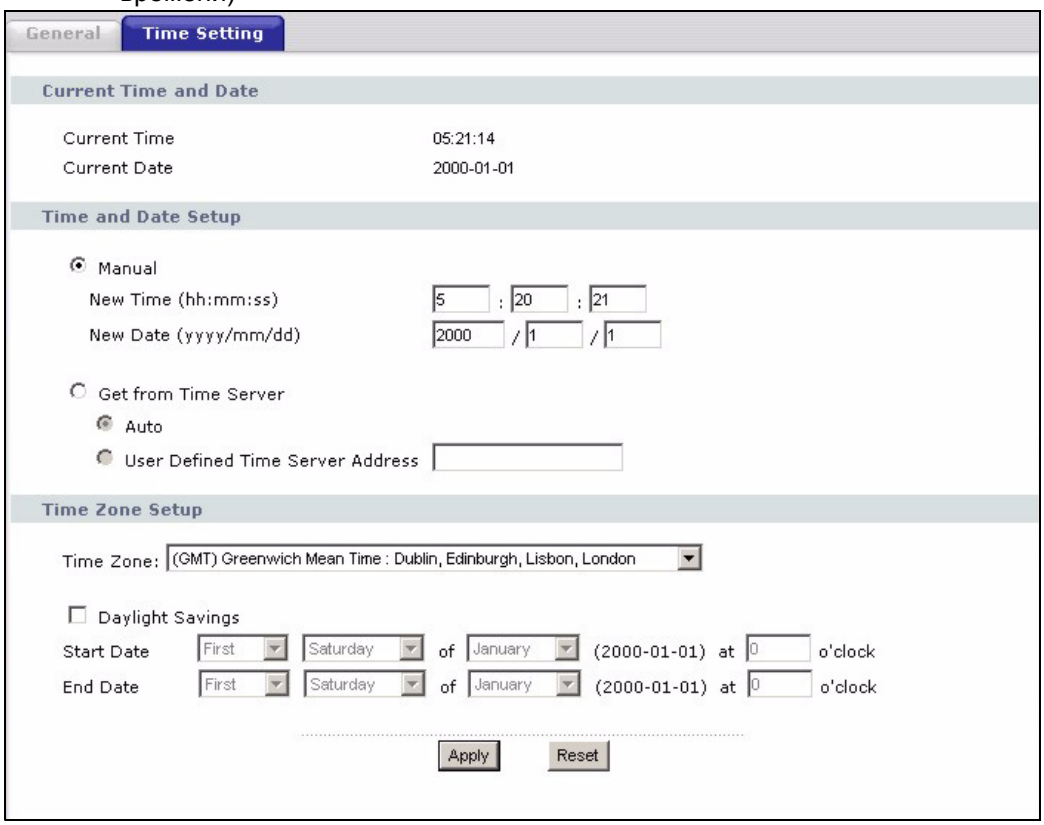
Табл. 52 Maintenance (Сопровождение) > System (Система) > General (Общие настройки)

ПОЛЕ	ОПИСАНИЕ
Administrator Inactivity Timer (Таймер простоя сеанса администрирования)	Введите время простоя в минутах, по истечении которого сеанс управления будет завершен. Значение по умолчанию 5 минут. Чтобы подключиться после завершения сеанса, необходимо снова зарегистрироваться и ввести пароль. Очень долгое время простоя увеличивает риск нарушения безопасности сети. Значение 0 означает, что сеанс управления не разрывается, независимо от времени простоя (не рекомендуется).
Password Setup (Настройка пароля)	С помощью этого поля рекомендуется сменить стандартный пароль интернет-центра NBG334W.
Old Password (Старый пароль)	Введите в данное поле пароль по умолчанию или текущий пароль, который используется для доступа к системе.
New Password (Новый пароль)	Введите новый системный пароль длиной до 30 символов. При вводе пароля каждый символ на экране отображается символом звездочки «*».
Retype to Confirm (Повторный ввод для подтверждения)	Введите в данное поле новый пароль еще раз.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

16.2 Окно установки времени

Для изменения даты и времени в NBG334W щелкните пункт **Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)**. При этом откроется следующее окно. Это окно используется для установки времени в интернет-центре NBG334W в соответствии с вашим часовым поясом.

Рис. 81 Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)



В следующей таблице даны описания полей этого окна.

Табл. 53 Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)

ПОЛЕ	ОПИСАНИЕ
Current Time and Date (Текущее время и дата)	
Current Time (Текущее время)	В этом поле отображается время в интернет-центре NBG334W. При каждой загрузке этой страницы интернет-центр NBG334W синхронизирует время с сервером времени.
Current Date (Текущая дата)	В этом поле отображается дата в интернет-центре NBG334W. При каждой загрузке этой страницы интернет-центр NBG334W синхронизирует дату с сервером времени.
Time and Date Setup (Установка времени и даты)	

Табл. 53 Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)

ПОЛЕ	ОПИСАНИЕ
Manual (Вручную)	Выберите эту опцию для установки времени и даты вручную. При одновременной установке новых параметров даты и времени, часового пояса и перехода на летнее время, новые дата и время имеют приоритет, и параметры **Time Zone (Часовой пояс)** и **Daylight Saving (Переход на летнее время)** не влияют на них.
New Time (Новое время) (hh:mm:ss) (чч:мм:сс)	В этом поле отображается время, последний раз обновленное с помощью сервера времени или последний раз установленное вручную. При выборе в разделе **Time and Date Setup (Установка времени и даты)** режима **Manual (Ручной)** введите в это поле новое время и щелкните по кнопке **Apply (Применить)**.
New Date (Новая дата) (yyyy/mm/dd) (гггг/мм/дд)	В этом поле отображается дата, последний раз обновленная с помощью сервера времени или последний раз установленная вручную. При выборе в разделе **Time and Date Setup (Установка времени и даты)** режима **Manual (Ручной)**, введите в это поле новую дату и нажмите кнопку **Apply (Применить)**.
Get from Time Server (Получить от сервера времени)	Выберите эту опцию, чтобы NBG334W синхронизировал время и дату с сервером, указанным в поле ниже.
Auto (Автоматически)	Вариант **Auto (Автоматически)** позволяет интернет-центру NBG334W самостоятельно выполнить поиск сервера времени и синхронизировать по нему свою дату и время.
User Defined Time Server Address (Адрес сервера времени задается пользователем)	Вариант **User Defined Time Server Address (Адрес сервера времени задается пользователем)** позволяет вручную указать IP-адрес или URL (длиной до 20 символов расширенного набора ASCII) сервера времени. Если нет уверенности в имеющейся информации, следует обратиться к Интернет-провайдеру или сетевому администратору.
Time Zone Setup (Установка часового пояса)	
Time Zone (Часовой пояс)	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time – GMT).
Daylight Savings (Переход на летнее время)	Летнее время – это период с поздней весны до ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток. Установите флажок, если вы используете переход на летнее время.

Табл. 53 Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)

ПОЛЕ	ОПИСАНИЕ
Start Date (Дата начала)	Введите месяц и день, когда начинается летнее время, если выбран вариант **Daylight Savings (Переход на летнее время)**. В поле **o'clock (час.)** используется 24 часовой формат. Далее приводится два примера: В большинстве частей Соединенных Штатов переход на летнее время начинается в первое воскресенье апреля. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **First (Первое), Sunday (Воскресенье), April (Апрель)** и 2 в поле **o'clock (часы)**. В странах Европейского Союза переход на летнее время начинается в последнее воскресенье марта. Во всех временных зонах Европейского Союза переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского союза необходимо установить **Last (Последнее), Sunday (Воскресенье), March (Март)**. Время, которое нужно ввести в поле **o'clock (часы)** зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).
End Date (Конечная дата)	Введите месяц и день, когда заканчивается летнее время, если выбран вариант **Daylight Savings (Переход на летнее время)**. В поле **o'clock (час.)** используется 24 часовой формат. Далее приводится два примера: В Соединенных Штатах летнее время заканчивается в последнее воскресенье октября. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **Last (Последнее), Sunday (Воскресенье), October (Октябрь)** и 2 в поле **o'clock (часы)**. В странах Европейского Союза летнее время заканчивается в последнее воскресенье октября. Во всех временных зонах Европейского Союза обратный переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского Союза необходимо установить **Last (Последнее), Sunday (Воскресенье), October (Октябрь)**. Время, которое нужно ввести в поле **o'clock (часы)** зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).
Apply (Применить)	Щелкните по кнопке **Apply (Применить)** для сохранения настроек NBG334W.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

17

Регистрационные журналы

В этой главе описывается настройка общих параметров регистрационных журналов, а также порядок просмотра журналов интернет-центра NBG334W. Примеры журнальных сообщений см. в приложениях.

17.1 Просмотр журнала регистрации

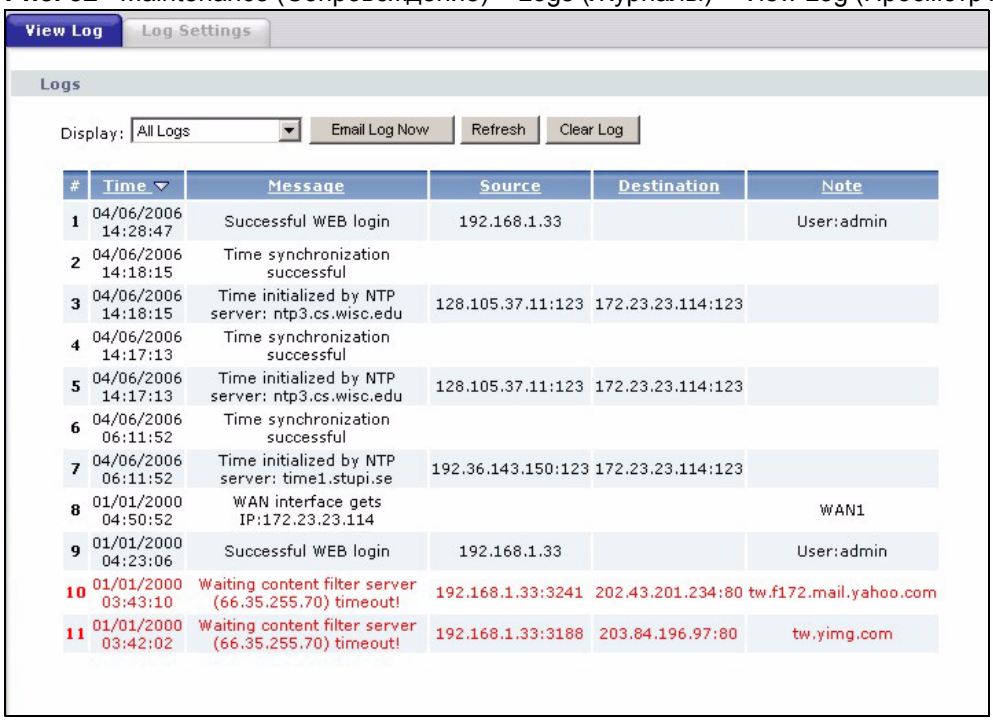
Веб-конфигуратор позволяет просматривать все журналы NBG334W в одном месте.

Щелкните **Maintenance (Сопровождение) > Logs (Регистрационные журналы)** для отображения окна **View Log (Просмотр журнала)**.

В окне **View Log (Просмотр журнала)** можно посмотреть журнальные записи по категориям, выбранным в окне **Log Settings (Настройки журналов)** (см. в Разд. 17.2 на с. 167). Можно просматривать журналы сопровождения системы, системных ошибок, контроля доступа, разрешенных или запрещенных веб-сайтов, запрещенных веб-функций (например, элементов управления ActiveX, Java и cookies), журналы атак (например, атак DoS) и IPSec.

Записи, отмеченные красным цветом сигнализируют о системных ошибках. Если журнал заполнен, самые старые журнальные записи стираются по мере добавления новых. Щелкните по заголовку столбца для сортировки записей. Треугольник показывает возрастающий или убывающий порядок сортировки.

Рис. 82 Maintenance (Сопровождение) > Logs (Журналы) > View Log (Просмотр журнала)



В следующей таблице даны описания полей этого окна.

Табл. 54 Maintenance (Сопровождение) > Logs (Журналы) > View Log (Просмотр журнала)

ПОЛЕ	ОПИСАНИЕ
Display (Отобразить)	Отображение категорий, выбранных на странице **Log Settings (Настройки журналов)** (см. Разд. 17.2 на с. 167), в выпадающем списке. Выберите категорию журналов для просмотра или установите **All Logs (Все журналы)** для просмотра журналов всех категорий, выбранных в окне **Log Settings (Настройки журналов)**.
Email Log Now (Отправить журнал по электронной почте)	Нажмите **Email Log Now (Отправить журнал по электронной почте)** для отправки журнала на адрес электронной почты, указанный в окне **Log Settings (Настройки журналов)** (в окне сначала нужно заполнить поле **Address Info (Информация об адресе)**).
Refresh (Обновить)	Нажмите **Refresh (Обновить)** для обновления экрана регистрационных записей.
Clear Log (Удалить записи)	Нажмите **Clear Log (Удалить записи)** для удаления всех регистрационных записей из журнала.
Time (Время)	В этом поле отображается время, когда была зарегистрирована запись. Инструкцию по настройке времени и даты на NBG334W см. в главе по сопровождению системы.
Message (Сообщение)	В этом поле приводится причина внесения записи в журнал.
Source (Источник)	В этом поле указываются IP-адрес источника и номер порта входящего пакета.
Destination (Получатель)	В этом поле указываются IP-адрес получателя и номер порта входящего пакета.
Note (Примечание)	В этом поле выводится дополнительная информация о регистрационной записи.

17.2 Настройка журналов

Настройка журналов интернет-центра NBG334W выполняется в одном месте.

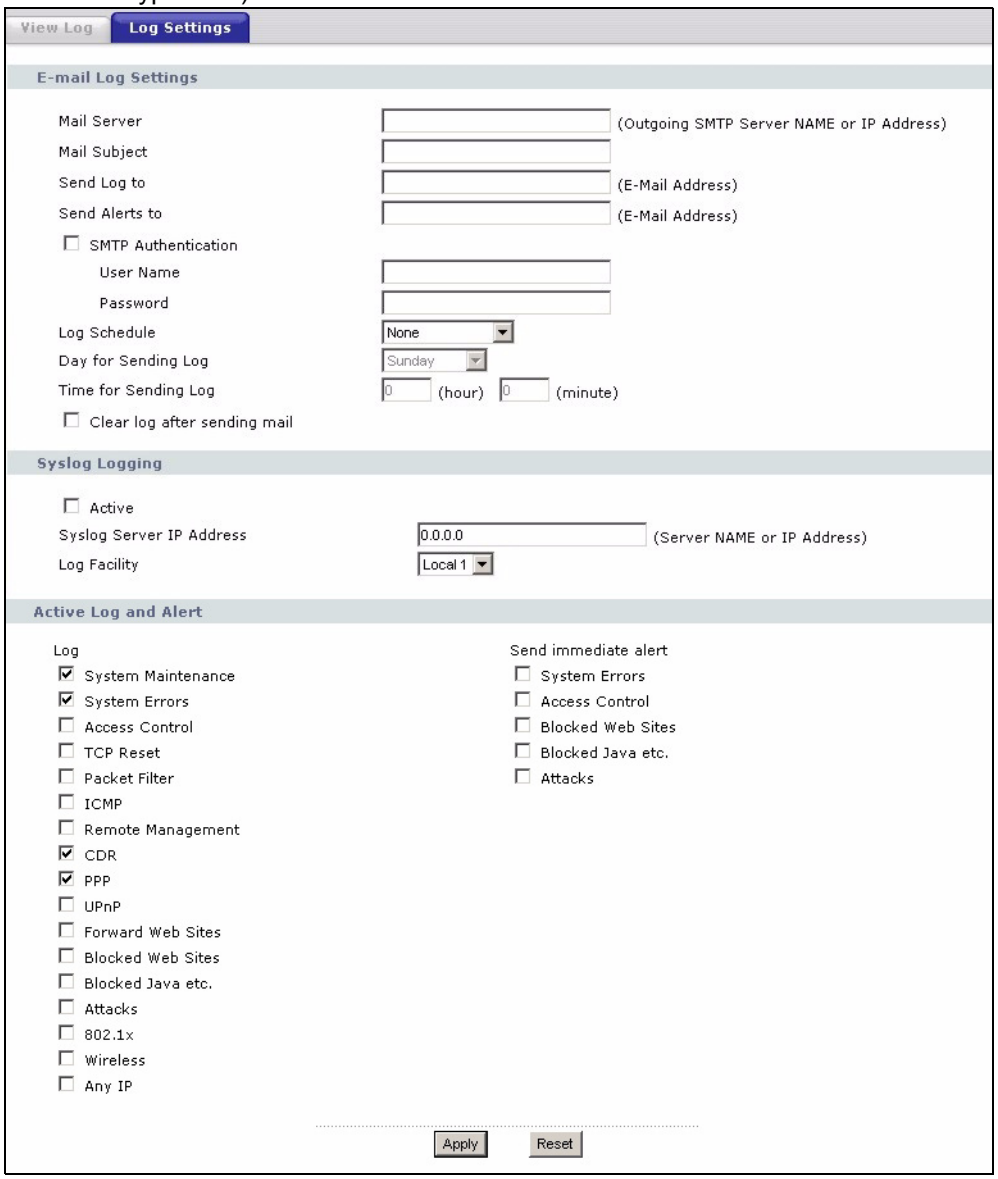
Для изменения настроек журналов щелкните **Maintenance (Сопровождение) > Logs (Регистрационные журналы) > Log Settings (Настройки журналов)**.

В окне **Log Settings (Настройки журналов)** можно установить следующие параметры: куда NBG334W должен отправлять журналы; расписание, когда NBG334W должен отправлять журналы и отправку каких журналов и/или срочных предупреждений NBG334W должен производить.

Предупреждение – это тип журнальной записи, требующий серьезного внимания. С помощью этих параметров настраивается обработка системных ошибок, атак (контроль доступа) и попыток доступа к запрещенным веб-сайтам или сайтам с запрещенными веб-функциями, например, cookies, active X и т.п. Некоторые категории, такие как **System Errors (Системные ошибки)** состоят как из журнальных записей, так и предупреждений. Вы можете различить их по цвету в окне **View Log (Просмотр журнала)**. Предупреждения отображаются красным цветом, а обычные журнальные записи – черным.

Предупреждения отправляются адресату непосредственно в момент их появления. Журналы отправляются по электронной почте по мере заполнения (см. раздел «**План журнальной регистрации**»). Выбор большого количества категорий предупреждений и/или журнальных записей (особенно это касается категории **Access Control (Управление доступом)**) может привести к тому, что будет рассылаться большое количество сообщений электронной почты.

Рис. 83 Maintenance (Сопровождение) > Logs (Журналы) > Log Settings (Настройки журналов)



В следующей таблице даны описания полей этого окна.

Табл. 55 Maintenance (Сопровождение) > Logs (Журналы) > Log Settings (Настройки журналов)

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings (Настройки журналов для отправки по электронной почте)	
Mail Server (Почтовый сервер)	Введите имя сервера или IP-адрес почтового сервера для указанных ниже адресов электронной почты. Если не заполнять это поле, журнал и предупреждающие сообщения не будут высылаться по электронной почте.
Mail Subject (Тема сообщения)	Введите заголовок для помещения в строку «subject» (тема) сообщения электронной почты, отправляемого NBG334W.
Send log to (Адресаты журнальных записей)	Интернет-центр NBG334W отправляет регистрационные журналы по адресам электронной почты, указанным в этом поле. Если это поле оставить пустым, NBG334W не отправляет журналы по электронной почте.

Табл. 55 Maintenance (Сопровождение) > Logs (Журналы) > Log Settings (Настройки журналов)

ПОЛЕ	ОПИСАНИЕ
Send alerts to (Адресаты предупреждений)	Предупреждения – это сообщения в реальном времени, посылаемые сразу после того, как произошло событие, такое как, атака DoS, системная ошибка или попытка доступа в запрещенную зону сети. Введите адрес электронной почты, куда будут отправляться предупреждающие сообщения. К предупреждающим сообщениям относятся сообщения о системных ошибках, атаках и попыткам доступа к заблокированным web-сайтам. Если это поле оставить пустым, предупреждающие сообщения не будут отправляться по электронной почте.
SMTP Authentication (Аутентификация на сервере SMTP)	SMTP (Simple Mail Transfer Protocol – Простой протокол электронной почты) – это стандартный протокол обмена сообщениями в сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой. Для включения аутентификации SMTP установите флажок в этом поле. Если требуется аутентификация почтового сервера, а эта функция выключена, вы не сможете получить журналы по электронной почте.
User Name (Имя пользователя)	Введите имя пользователя длиной до 31 символа (обычно это имя пользователя почтовой учетной записи).
Password (Пароль)	Введите пароль для данного имени пользователя.
Log Schedule (План журнальной регистрации)	В этом выпадающем меню выбирается частота рассылки журнальных записей по электронной почте: • Daily (Ежедневно) • Weekly (Еженедельно) • Hourly (Каждый час) • When Log is Full (По заполнении журнала) • None (Никогда). При выборе опции **Weekly (Еженедельно)** или **Daily (Ежедневно)** необходимо указать время дня для рассылки e-mail сообщений. При выборе опции **Weekly (Еженедельно)** также необходимо указать день недели для рассылки сообщений. При выборе опции **When Log is Full (По заполнении журнала)** сообщение посылается только при условии, что журнал заполнен. При выборе **None (Никогда)** сообщения не отправляются.
Day for Sending Log (День рассылки журнальных записей)	Из раскрывающегося списка выберите день недели, в который должны отправляться записи.
Time for Sending Log (Время рассылки журнальных записей)	Введите время отправки журнальных записей в 24-часовом формате (например, 23:00 для 11 часов вечера).
Clear log after sending mail (Очищать журнал после отправки почтовых сообщений)	Установите здесь флажок для удаления всех записей после их отправки интернет-центром NBG334W по электронной почте.
Syslog Logging (Системный журнал)	NBG334W отправляет журнал на внешний сервер системного журнала.
Active (Активировать)	Для активации системного журнала нажмите кнопку **Active (Активировать)**.

Табл. 55 Maintenance (Сопровождение) > Logs (Журналы) > Log Settings (Настройки журналов)

ПОЛЕ	ОПИСАНИЕ
Syslog Server IP Address (IP-адрес сервера системных журналов)	Введите имя сервера или IP-адрес сервера системных журналов, который будет регистрировать выбранные категории сообщений.
Log Facility (Размещение журнала)	Из выпадающего списка выберите место, где будут храниться журнальные записи. Эта функция дает возможность регистрировать сообщения в различных файлах на сервере системных журналов. Для получения дополнительной информации см. руководство по серверу системных журналов.
Active Log and Alert (Включить журналы и предупреждения)	
Log (Регистрационный журнал)	Выберите категории журнальных записей, которые необходимо регистрировать.
Send Immediate Alert (Отправить предупреждение немедленно)	Выберите категории журналов, для которых NBG334W будет отправлять предупреждения по электронной почте немедленно.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Reset (Сброс)	Нажмите **Reset (Сброс)**, чтобы начать настройку заново.

17.3 Описание сообщений журнала

В данном разделе приводится описание примеров сообщений в регистрационном журнале.

Табл. 56 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
`Time calibration is successful`	Маршрутизатор синхронизировал свое время на базе информации, полученной от сервера времени.
`Time calibration failed`	При синхронизации времени маршрутизатора с сервером времени произошел сбой.
`WAN interface gets IP:%s`	Интерфейсу WAN назначен новый IP-адрес от сервера DHCP, PPPoE, PPTP или удаленного сервера.
`DHCP client IP expired`	Время аренды IP-адреса клиента DHCP истекло.
`DHCP server assigns %s`	Сервер DHCP назначил клиенту IP-адрес.
`Successful WEB login`	Успешный вход в систему через интерфейс Web-конфигуратора.
`WEB login failed`	Произошел сбой при входе в систему через интерфейс Web-конфигуратора.
`Successful TELNET login`	Успешный вход в систему по telnet.
`TELNET login failed`	Произошел сбой при входе в систему по telnet.
`Successful FTP login`	Успешный вход в систему по ftp.
`FTP login failed`	Произошел сбой при регистрации сеанса ftp.

Табл. 56 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
NAT Session Table is Full!	Достигнуто максимальное число записей в таблице NAT и таблица заполнена.
Starting Connectivity Monitor	Запуск Диспетчера соединений.
Time initialized by Daytime Server	Маршрутизатор получил время и дату от сервера даты и времени.
Time initialized by Time server	Маршрутизатор получил время и дату от сервера времени.
Time initialized by NTP server	Маршрутизатор получил время и дату от сервера NTP.
Connect to Daytime server fail	Произошел сбой при подключении маршрутизатора к серверу даты и времени.
Connect to Time server fail	Произошел сбой при подключении маршрутизатора к серверу времени.
Connect to NTP server fail	Произошел сбой при подключении маршрутизатора к серверу NTP.
Too large ICMP packet has been dropped	Маршрутизатор сбросил пакет ICMP, размер которого превышал допустимый.
Configuration Change: PC = 0x%x, Task ID = 0x%x	Маршрутизатор сохраняет изменения конфигурации.
Successful SSH login	Успешный вход в систему через сервер SSH.
SSH login failed	Произошел сбой при входе в систему через сервер SSH маршрутизатора.
Successful HTTPS login	Успешный вход в систему через интерфейс Web-конфигуратора по протоколу HTTPS.
HTTPS login failed	Произошел сбой при входе в систему через интерфейс Web-конфигуратора по протоколу HTTPS.

Табл. 57 Журнальные сообщения о системных ошибках

СООБЩЕНИЕ	ОПИСАНИЕ
%s exceeds the max. number of session per host!	Попытка создания сеанса NAT привела к превышению максимального количества записей в таблице сеансов NAT, допустимого для одного узла.
setNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
readNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
WAN connection is down.	Подключение к глобальной сети не работает. Доступ в сеть через этот интерфейс невозможен.

Табл. 58 Журнальные сообщения, связанные с управлением доступом

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Попытка доступа через протокол TCP/UDP/IGMP/ESP/ GRE/OSPF, подпадающая под действие политики межсетевого экрана, заданной по умолчанию, и заблокированная либо переадресованная согласно установкам этой политики.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>`	Попытка доступа через протокол TCP/UDP/IGMP/ESP/ GRE/OSPF, подпадающая (или не подпадающая) под действие заданного правила межсетевого экрана (обозначается номером) и заблокированная или переадресованная согласно этому правилу.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
`Router sent blocked web site message: TCP`	Маршрутизатор отправил сообщение, уведомляющее пользователя о блокировке доступа к запрошенному Web-сайту.

Табл. 59 Журнальные сообщения о сбросе сеансов TCP

СООБЩЕНИЕ	ОПИСАНИЕ
`Under SYN flood attack, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP при обнаружении синхронной атаки на узел (подсчет незавершенных сеансов TCP ведется по целевому узлу).
`Exceed TCP MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество открытых соединений TCP превысило заданное пользователем пороговое значение. (Подсчет открытых сеансов TCP ведется по целевому узлу). Примечание: информацию о значении порога **TCP Maximum Incomplete (Максимум неполных TCP)** см. в описании окна **Firewall Attack Alerts (Предупреждения об атаках на межсетевой экран)**.
`Peer TCP state out of order, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда состояние TCP соединения было неисправно. Примечание: межсетевой экран проверяет состояние TCP по RFC793 Рис. 6.
`Firewall session time out, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP по истечении времени простоя динамического сеанса связи через межсетевой экран. Время простоя сеансов связи по умолчанию: Время простоя сеанса ICMP: 3 минуты Время простоя сеанса UDP: 3 минуты Время ожидания соединения TCP (трехстороннее согласование установления связи): 270 секунд Время ожидания FIN-пакета TCP: 2 MSL (значение **Maximum Segment Lifetime (Максимальная продолжительность сегмента)**, установленное в заголовке TCP). Время простоя установленного соединения TCP: 150 минут Время ожидания сброса TCP соединения: 10 секунд

Табл. 59 Журнальные сообщения о сбросе сеансов TCP (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Exceed MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество открытых соединений (через TCP и UDP) превысило заданное пользователем пороговое значение (Подсчет незавершенных подключений производится для всех подключений по TCP и UDP через межсетевой экран.) Примечание: когда количество незавершенных подключений (TCP + UDP) превышает верхний порог («Maximum Incomplete High»), маршрутизатор отправляет пакеты сброса (TCP RST) подключений через TCP и начинает удаление динамических сеансов связи через межсетевой экран (TOS); операция прекращается, когда количество незавершенных подключений становится меньше нижнего порога («Maximum Incomplete Low»).
`Access block, sent TCP RST`	Маршрутизатор отправляет пакет TCP RST и создает эту запись в журнале, если включен механизм сброса TCP межсетевого экрана (с помощью команды интерпретатора «sys firewall tcprst»).

Табл. 60 Журнальные сообщения о фильтре пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Произведена попытка доступа, соответствующая настроенному правилу фильтра (указывается номер набора и номер правила), и выполнена блокировка или пересылка пакета в соответствии с правилом.

Табл. 61 Журнальные сообщения ICMP (Протокол межсетевых управляющих сообщений)

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	Доступ через протокол межсетевых управляющих сообщений (ICMP), подпадающий под действие политики по умолчанию и заблокированный или переадресованный согласно настройкам пользователя. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	Доступ через ICMP, подпадающий (либо не подпадающий) под действие правила для межсетевых экранов (идентифицированное своим номером) и блокированный или переадресованный в соответствии с правилом. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
`Triangle route packet forwarded: ICMP`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.
`Packet without a NAT table entry blocked: ICMP`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
`Unsupported/out-of-order ICMP: ICMP`	Межсетевой экран не поддерживает такие пакеты ICMP либо произошел сбой в пакетах ICMP.
`Router reply ICMP packet: ICMP`	Маршрутизатор послал ответный пакет ICMP отправителю.

Табл. 62 Журнальные сообщения CDR (Журнала регистрации вызовов)

СООБЩЕНИЕ	ОПИСАНИЕ
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	Маршрутизатор получил запрос на установление соединения для выполнения вызова. «call» – номер вызова. «dev» – тип устройства (3 – коммутируемое соединение, 6 – PPPoE, 10 – PPTP). «channel» или «ch» – идентификатор канала вызова. Например, «board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0» означает, что маршрутизатор выполнял вызов сервера PPPoE 3 раза.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	Установлено PPPoE, PPTP или коммутируемое соединение.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	Прервано PPPoE, PPTP или коммутируемое соединение.

Табл. 63 Журнальные сообщения PPP (Протокол «точка-точка»)

СООБЩЕНИЕ	ОПИСАНИЕ
`ppp:LCP Starting`	Запущена стадия протокола управления каналом связи для PPP соединения.
`ppp:LCP Opening`	Открывается стадия протокола управления каналом связи для PPP соединения.
`ppp:CHAP Opening`	Открывается стадия протокола аутентификации по методу «Challenge Handshake Authentication» (Вызов-рукопожатие) для PPP соединения.
`ppp:IPCP Starting`	Начинается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:IPCP Opening`	Открывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:LCP Closing`	Закрывается стадия протокола управления каналом связи (Link Control Protocol) для PPP соединения.
`ppp:IPCP Closing`	Закрывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.

Табл. 64 Журнальные сообщения UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
`UPnP pass through Firewall`	Пакеты UPnP могут проходить через межсетевой экран.

Табл. 65 Журнальные сообщения о фильтрации содержимого

СООБЩЕНИЕ	ОПИСАНИЕ
`%s: Keyword blocking`	На запрошенной веб-странице имеется заданное пользователем ключевое слово.
`%s: Not in trusted web list`	Данный web-сайт находится на домене, не гарантирующем высокой степени защиты, и маршрутизатор блокирует весь трафик, оставляя доступ только к сайтам, размещенным на надежных доменах.
`%s: Forbidden Web site`	Данный web-сайт входит в список запрещенных.
`%s: Contains ActiveX`	Данный web-сайт содержит элементы ActiveX.
`%s: Contains Java applet`	Данный web-сайт содержит апплеты языка Java.
`%s: Contains cookie`	Данный web-сайт содержит файлы cookie.
`%s: Proxy mode detected`	Маршрутизатор обнаружил режим proxy в данном пакете.
`%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, но не указал категорию блокировки.
`%s:%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, и указал категорию блокировки.
`%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, но не указала категорию блокировки.
`%s:%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, и известна категория блокировки.
`%s: Trusted Web site`	Данный web-сайт находится на доверенном домене с высокой степенью защиты.
`%s`	Если фильтр содержания отключен согласно расписанию или Вы не установили флажок «Block Matched Web Site» (Блокируемый сайт), то система переадресует содержание.
`Waiting content filter server timeout`	Сервер фильтрации внешнего содержания не ответил в течение заданного времени ожидания.
`DNS resolving failed`	Интернет-центр NBG334W не может получить IP-адрес сервера фильтрации внешнего контента с помощью запроса DNS.
`Creating socket failed`	Интернет-центр NBG334W не может создать запрос из-за сбоя при создании канала TCP/IP, порт:номер порта.
`Connecting to content filter server fail`	Сбой при подключении к серверу фильтрации внешнего содержания.
`License key is invalid`	Недействительный лицензионный ключ внешнего сервера фильтрации содержания.

Табл. 66 Журнальные сообщения об атаках

СООБЩЕНИЕ	ОПИСАНИЕ
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран обнаружил атаку TCP/UDP/IGMP/ESP/GRE/OSPF.
attack ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку ICMP. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран обнаружил атаку по TCP/UDP/IGMP/ESP/GRE/OSPF на каталог локальной сети (LAND).
land ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку ICMP на каталог локальной сети (LAND). Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран обнаружил атаку с подменой IP-адреса на порт WAN.
ip spoofing - WAN ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку с подменой IP-адреса ICMP на порт WAN. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
icmp echo: ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку с использованием отклика ICMP. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
syn flood TCP	Межсетевой экран обнаружил синхронную атаку TCP.
ports scan TCP	Межсетевой экран обнаружил атаку TCP со сканированием портов.
teardrop TCP	Межсетевой экран обнаружил Teardrop-атаку TCP.
teardrop UDP	Межсетевой экран обнаружил Teardrop-атаку UDP.
teardrop ICMP (type:%d, code:%d)	Межсетевой экран обнаружил Teardrop-атаку ICMP. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
illegal command TCP	Межсетевой экран обнаружил атаку TCP с недопустимой командой.
NetBIOS TCP	Межсетевой экран обнаружил атаку TCP NetBIOS.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран классифицировал пакет без записи о маршрутизации от источника как атаку с подменой IP-адреса.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	Межсетевой экран классифицировал пакет ICMP без указания источника как атаку с подстановкой IP (IP spoofing).
vulnerability ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку ICMP на уязвимость. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.
traceroute ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку ICMP с отслеживанием маршрута. Подробное описание типов и кодов приведено в Табл. 70 на с. 180.

Табл. 67 Журнальные сообщения PKI (Инфраструктура сертификации открытых ключей)

СООБЩЕНИЕ	ОПИСАНИЕ
`Enrollment successful`	Успешно выполнена регистрация сертификата SCEP в режиме реального времени. Поле **Destination (Адрес назначения)** содержит IP-адрес и порт сервера центра сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени. Поле **Destination (Адрес назначения)** содержит IP-адрес и порт сервера центра сертификации.
`Failed to resolve <SCEP CA server url>`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени из-за невозможности определения адреса сервера бюро сертификации.
`Enrollment successful`	Успешно выполнена регистрация сертификата CMP в режиме реального времени. Поле **Destination (Адрес назначения)** содержит IP-адрес и порт сервера центра сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени. Поле **Destination (Адрес назначения)** содержит IP-адрес и порт сервера центра сертификации.
`Failed to resolve <CMP CA server url>`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени из-за невозможности определения IP-адреса сервера бюро сертификации.
`Rcvd ca cert: <subject name>`	Маршрутизатор получил сертификат бюро сертификации с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Rcvd user cert: <subject name>`	Маршрутизатор получил сертификат пользователя с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Rcvd CRL <size>: <issuer name>`	Маршрутизатор получил список аннулирования сертификатов (CRL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Rcvd ARL <size>: <issuer name>`	Маршрутизатор получил список аннулирования полномочий (ARL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Failed to decode the received ca cert`	Маршрутизатор получил недействительный сертификат центра сертификации от сервера LDAP, IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Failed to decode the received user cert`	Маршрутизатор получил недействительный сертификат пользователя от сервера LDAP, IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Failed to decode the received CRL`	Маршрутизатор получил недействительный список аннулирования сертификатов (CRL) от сервера LDAP, IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Failed to decode the received ARL`	Маршрутизатор получил недействительный список аннулирования полномочий (ARL) от сервера LDAP, IP-адрес и порт которого указаны в поле **Source (Отправитель)**.
`Rcvd data <size> too large! Max size allowed: <max size>`	Маршрутизатор получил слишком большой объем данных справочника (с указанием размера) от сервера LDAP, IP-адрес и порт которого указаны в поле **Source (Отправитель)**. Также указывается максимальный размер данных справочника, которые может пропустить маршрутизатор.

Табл. 67 Журнальные сообщения PKI (Инфраструктура сертификации открытых ключей) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Cert trusted: <subject name>`	Маршрутизатор сверил путь сертификата с указанной темой.
`Due to <reason codes>, cert not trusted: <subject name>`	В силу перечисленных причин сертификат с указанной темой не прошел сверку пути. Зарегистрированные коды отражают лишь примерные причины ненадежности сертификату. Соответствующие описания кодов приведены в Табл. 70 на с. 180.

Табл. 68 Журнальные сообщения 802.1X

СООБЩЕНИЕ	ОПИСАНИЕ
`Local User Database accepts user.`	Подлинность пользователя была установлена встроенной базой данных пользователей.
`Local User Database reports user credential error.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как был введен неверный пароль.
`Local User Database does not find user`s credential.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как пользователь не числится во встроенной базе данных.
`RADIUS accepts user.`	Подлинность пользователя была установлена сервером RADIUS.
`RADIUS rejects user. Pls check RADIUS Server.`	Подлинность пользователя не была установлена сервером RADIUS. Проверьте сервер RADIUS.
`Local User Database does not support authentication method.`	Встроенная база данных пользователей поддерживает только метод EAP-MD5. Пользователь пытался использовать другой метод аутентификации и его подлинность не была установлена.
`User logout because of session timeout expired.`	Маршрутизатор вывел из системы пользователя с истекшим сроком действия сеанса связи.
`User logout because of user deassociation.`	Маршрутизатор вывел из системы пользователя, завершившего сеанс связи.
`User logout because of no authentication response from user.`	Маршрутизатор вывел из системы пользователя, от которого не поступил ответ на аутентификацию.
`User logout because of idle timeout expired.`	Маршрутизатор вывел из системы пользователя, у которого превышен лимит времени простоя.
`User logout because of user request.`	Пользователь вышел из системы.
`Local User Database does not support authentication method.`	Пользователь попытался использовать метод аутентификации, не поддерживаемый встроенной базой данных пользователей (база поддерживает только EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	Нет ответа от сервера RADIUS, проверьте сервер RADIUS.
`Use Local User Database to authenticate user.`	Встроенная база данных пользователей работает в качестве аутентификационного сервера.
`Use RADIUS to authenticate user.`	Сервер RADIUS работает в качестве аутентификационного сервера.

Табл. 68 Журнальные сообщения 802.1X (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`No Server to authenticate user.`	Отсутствует аутентификационный сервер, способный установить подлинность пользователя.
`Local User Database does not find user`s credential.`	Подлинность пользователя не была установлена встроенной базой данных пользователей, так как пользователь не числится во встроенной базе данных.

Табл. 69 Настройка списка управления доступом (ACL)

НАПРАВЛЕНИЕ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	LAN to WAN (лок. сеть – глоб. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из локальной сети (LAN) в глобальную (WAN).
(W to L)	WAN to LAN (глоб. сеть – лок. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из глобальной сети (WAN) в локальную (LAN).
(L to L/P)	LAN to LAN/ NBG334W (локальная сеть – локальная сеть/ ZyXEL P-662)	Список управления доступом (ACL) для пакетов, пересылаемых из одной локальной сети (LAN) в другую локальную сеть (LAN) или в NBG334W.
(W to W/P)	WAN to WAN/ NBG334W (глобальная сеть – глобальная сеть/ ZyXEL P-662)	Список управления доступом (ACL) для пакетов, пересылаемых из одной глобальной сети в другую или в NBG334W.

Табл. 70 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение с эхо-ответом
3		Адресат недоступен
	0	Сеть недоступна
	1	Узел недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, который требует фрагментации, отброшен, так как имеет параметр DF (Don't Fragment – не фрагментировать)
	5	Ошибка в маршруте источника
4		Источник произвел сброс
	0	Шлюз может сбросить дейтаграммы Интернет, если он не имеет буферной памяти, достаточной для организации очереди дейтаграмм, чтобы передать их в следующую сеть по маршруту к сети получателя.
5		Перенаправление
	0	Перенаправление дейтаграмм для сети
	1	Перенаправление дейтаграмм для узла
	2	Перенаправление дейтаграмм для типа услуги (ToS) и сети
	3	Перенаправление дейтаграмм для типа услуги (ToS) и узла
8		Эхо
	0	Эхо-сообщение
11		Время истекло
	0	Время жизни пакета истекло в пути
	1	Время на повторную сборку фрагментов истекло
12		Неверный параметр
	0	Указатель показывает на ошибку
13		Временная метка
	0	Сообщение с запросом временной метки
14		Ответ с временной меткой
	0	Ответное сообщение с временной меткой
15		Запрос параметров
	0	Сообщение с запросом параметров
16		Ответ на запрос параметров
	0	Сообщение с ответом на запрос параметров

Табл. 71 Сообщения системного журнала

СООБЩЕНИЕ	ОПИСАНИЕ
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	Это сообщение посылается системой («RAS» отображается в качестве системного имени, если оно не было присвоено), когда маршрутизатор создает запись в системном журнале. Эта функция устанавливается на странице: ГЛАВНОЕ МЕНЮ Web-конфигуратора->ЖУРНАЛЫ РЕГИСТРАЦИИ->Настройки журналов. Серьезность ошибки – это класс записи в системном журнале. Описание сообщений и записей определяются различными схемами записей в этом приложении. «devID» – это последние три символа MAC-адреса порта LAN маршрутизатора. «cat» – то же, что категория в журналах маршрутизатора.

В следующей таблице приводятся типы полезной информации в сообщениях протокола ISAKMP (см. RFC-2408), и их обозначения в журнале. Более подробную информацию по каждому типу см. в RFC.

Табл. 72 Типы данных сообщений RFC-2408 ISAKMP

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ПОЛЕЗНОЙ ИНФОРМАЦИИ
SA	Безопасное соединение
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Сигнатура
NONCE	Сл. число
NOTFY	Уведомление
DEL	Удалить
VID	Идентификационный номер поставщика

Программные средства

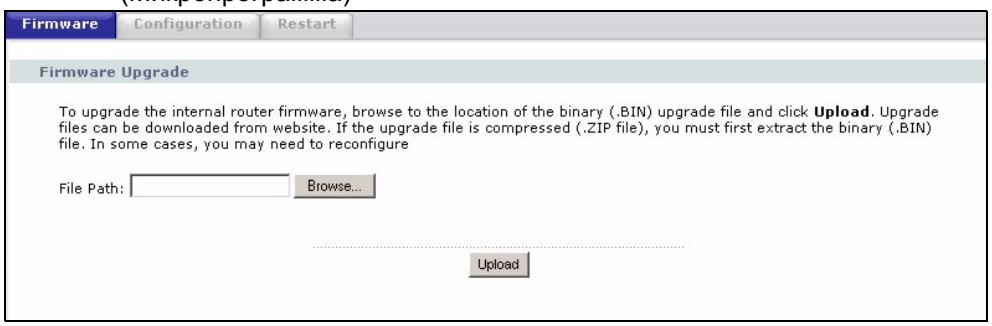
В данной главе описываются процедуры загрузки новой микропрограммы, выгрузки или сохранения резервной копии файлов конфигурации и перезапуска интернет-центра NBG334W.

18.1 Окно загрузки микропрограммы

Найдите микропрограмму на сайте www.zyxel.com в файле, в названии которого обычно использовано название модели с расширением «*.bin» extension, например, «NBG334W.bin». Для загрузки используется протокол HTTP (Hypertext Transfer Protocol – Протокол передачи гипертекста), загрузка может занять до 2-х минут. После успешной загрузки микропрограммы система перезапускается. Информацию по обновлению микропрограммы с помощью команд FTP/TFTP см. в главе «Сопровождение микропрограммы и файла конфигурации».

Выберите пункт **Maintenance (Сопровождение) > Tools (Инструменты)**. Следуйте указаниям в этом окне для загрузки микропрограммы в интернет-центр NBG334W.

Рис. 84 Maintenance (Сопровождение) > Tools (Программные средства) > Firmware (Микропрограмма)



В следующей таблице даны описания полей этого окна.

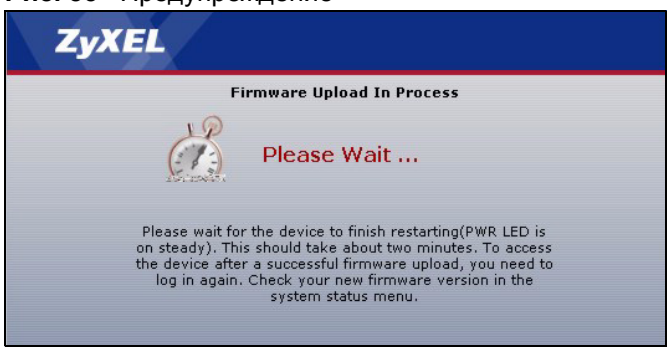
Табл. 73 Maintenance (Сопровождение) > Tools (Программные средства) > Firmware (Микропрограмма)

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите путь к файлу, который требуется загрузить, или нажмите кнопку **Browse... (Обзор)**, чтобы выполнить поиск файла.
Browse... (Обзор...)	Нажмите кнопку **Browse (Просмотр)**,чтобы указать местонахождение файла с расширением .bin, который вы хотите загрузить. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Upload (Загрузка)	Нажмите кнопку **Upload (Загрузка)** для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.

НЕЛЬЗЯ выключать питание NBG334W во время загрузки микропрограммы!

После появления окна **Firmware Upload in Progress (Выполняется загрузка микропрограммы)**, подождите 2 минуты, прежде чем снова регистрироваться в NBG334W.

Рис. 85 Предупреждение



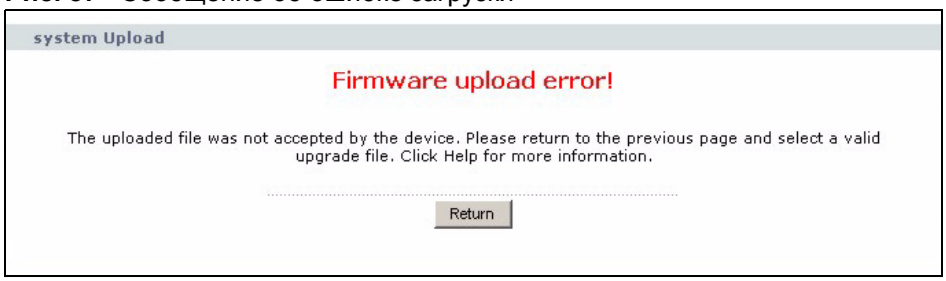
NBG334W автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах на рабочем столе может появиться следующий значок:

Рис. 86 Временное отключение сети

По истечении 2 минут снова зарегистрируйтесь и проверьте версию новой микропрограммы в окне **System Status (Состояние системы)**.

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку **Return (Возврат)** для возврата к окну **Firmware (Микропрограмма)**.

Рис. 87 Сообщение об ошибке загрузки

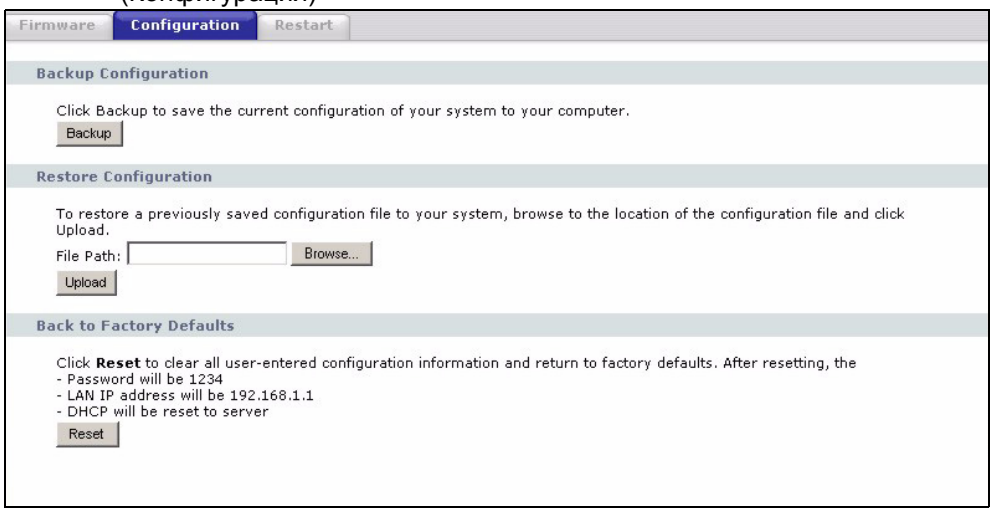


18.2 Окно конфигурации

Информацию по переносу файлов конфигурации с помощью команд FTP/TFTP см. в главе «Сопровождение микропрограммы и файла конфигурации».

Щелкните **Maintenance (Сопровождение) > Tools (Программные средства) > Configuration (Конфигурация)**. В этом окне отображается информация о заводских настройках по умолчанию, резервном сохранении и восстановлении конфигурации.

Рис. 88 Maintenance (Сопровождение) > Tools (Программные средства) > Configuration (Конфигурация)



18.2.1 Резервное сохранение конфигурации

Резервное сохранение конфигурации позволяет сохранить текущую конфигурацию NBG334W в файле на компьютере. Если настройка NBG334W выполнена, и устройство работает нормально, то перед внесением каких-либо изменений настоятельно рекомендуется создать резервную копию файла конфигурации. Файл с резервной копией конфигурации пригодится в случае, если Вам придется вернуться к предыдущим настройкам.

Для сохранения текущей конфигурации NBG334W на компьютере щелкните **Backup (Резервное сохранение)**.

18.2.2 Восстановление конфигурации

Функция восстановления конфигурации позволяет загрузить с компьютера в NBG334W новый или предварительно сохраненный файл конфигурации.

Табл. 74 Сопровождение: Восстановление конфигурации

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите путь к файлу, который вы хотите загрузить, или нажмите кнопку **Browse... (Обзор...)**, чтобы указать местонахождение файла.
Browse... (Обзор...)	Нажмите **Browse... (Обзор...)**, чтобы найти файл для загрузки. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Upload (Загрузка)	Нажмите кнопку **Upload (Загрузка)** для запуска процесса загрузки.

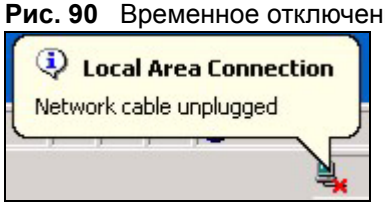
НЕЛЬЗЯ выключать питание NBG334W во время загрузки файла конфигурации!

После появления окна **Restore Configuration successful (Конфигурация успешно восстановлена)**, необходимо подождать одну минуту, прежде чем снова регистрироваться в NBG334W.

Рис. 89 Конфигурация успешно восстановлена

NBG334W автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах на рабочем столе может появиться следующий значок:

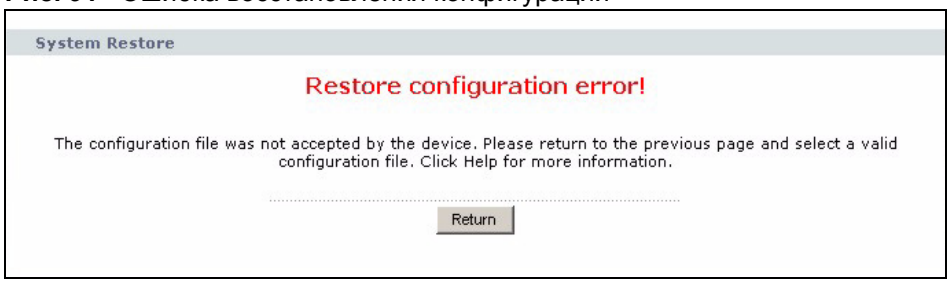
Рис. 90 Временное отключение сети



При загрузке файла конфигурации по умолчанию необходимо изменить IP-адрес компьютера, чтобы он находился в той же подсети, что и IP-адрес NBG334W по умолчанию (192.168.1.1). Подробнее об установке IP-адреса компьютера см. в кратком руководстве пользователя.

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку **Return (Возврат)** для возврата к окну **Configuration (Конфигурация)**.

Рис. 91 Ошибка восстановления конфигурации



18.2.3 Восстановление заводских настроек по умолчанию

При нажатии кнопки **Reset (Сброс)** в этом разделе сбрасываются все измененные пользователем параметры, и настройки NBG334W возвращаются к заводским настройкам по умолчанию.

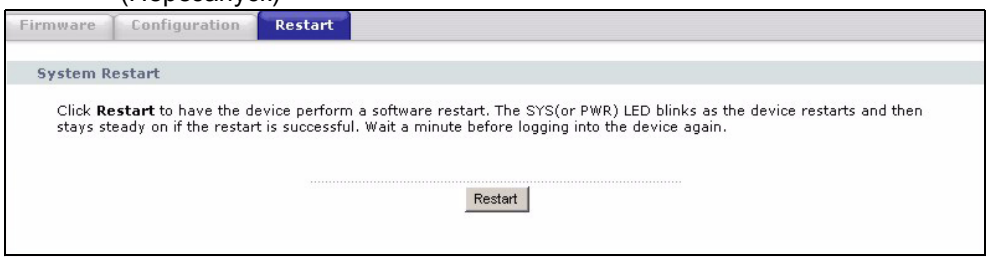
Восстановление заводских настроек NBG334W также можно выполнить, нажав кнопку **RESET (СБРОС)** на задней панели устройства. Дополнительную информацию о кнопке **RESET (СБРОС)** см. в главе описания Web-конфигуратора.

18.3 Окно Restart (Перезапуск)

Это окно позволяет выполнить перезагрузку NBG334W без выключения электропитания.

Щелкните **Maintenance (Сопровождение) > Tools (Программные средства) > Restart (Перезапуск)**. Нажмите кнопку **Restart (Перезапуск)** для перезапуска интернет-центра NBG334W. Эта операция не влияет на конфигурацию NBG334W.

Рис. 92 Maintenance (Сопровождение) > Tools (Программные средства) > Restart (Перезапуск)



19

Поиск и устранение неисправностей

В этой главе рассказывается об устранении возможных неисправностей, которые могут появиться при работе с устройством. Возможные неисправности можно разделить на следующие категории:

- Питание, подключение оборудования и светодиоды
- Доступ и регистрация в NBG334W
- Доступ в Интернет
- Восстановление заводских настроек NBG334W
- Поиск и устранение неисправностей беспроводного маршрутизатора и точки доступа
- Дополнительные функции

19.1 Питание, подключение оборудования и светодиоды

? Интернет-центр NBG334W не включается. Ни один из светодиодов не включается.

1. Убедитесь, что используется адаптер питания из комплекта поставки NBG334W.
2. Убедитесь, что адаптер питания подключен к NBG334W и домашней электросети.
3. Отключите и снова подключите к NBG334W адаптер питания.
4. Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

? Один из светодиодов работает неправильно.

1. Убедитесь, что вы знаете, как светодиод должен работать в нормальном режиме. См. Разд. 1.4 на с. 15.
2. Проверьте подключение оборудования. См. Краткое руководство.
3. Убедитесь, что кабели не повреждены. Для замены поврежденных кабелей свяжитесь с поставщиком оборудования.

4 Отключите и снова подключите к NBG334W адаптер питания.
5 Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

19.2 Доступ и регистрация в NBG334W

Потеряна информация об IP-адресе NBG334W.

1 IP-адрес, установленный изготовителем по умолчанию – **192.168.1.1**.
2 Если IP-адрес был изменен и затем информация об этом утеряна, можно посмотреть IP-адрес NBG334W, установленный для шлюза по умолчанию на компьютере. Чтобы выполнить это на компьютере под управлением Windows, нажмите кнопку **Start (Пуск) > Run (Выполнить)**, введите команду **cmd** и затем **ipconfig**. IP-адрес **Default Gateway (Шлюз по умолчанию)** может являться IP-адресом интернет-центра NBG334W (это зависит от конкретной сети). Введите этот IP-адрес в Интернет браузере.
3 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 19.4 на с. 193.

Утерян пароль.

1 По умолчанию установлен пароль **1234**.
2 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 19.4 на с. 193.

Не отображается окно Web-конфигуратора **Login (Вход в систему)** или отсутствует доступ в систему.

1 Убедитесь, что используется правильный IP-адрес.
   - IP-адрес, установленный изготовителем по умолчанию – 192.168.1.1.
   - Если IP-адрес был изменен (Разд. 6.3 на с. 80), используйте новый IP-адрес.
   - Если IP-адрес был изменен и затем утерян, см. рекомендации по поиску и устранению неисправностей в разделе Потеряна информация об IP-адресе NBG334W.
2 Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство.
3 Убедитесь, что в Интернет-браузере включена поддержка всплывающих окон, а также JavaScripts Java. См. Прил. B на с. 205.

4 Ваш компьютер должен находиться в той же подсети, что и интернет-центр NBG334W. (Пропустите этот шаг, если известно, что между компьютером и интернет-центром NBG334W имеются маршрутизаторы.)
   - Если в вашей сети есть сервер DHCP, убедитесь, что ваш компьютер использует динамический IP-адрес. См. Разд. 6.3 на с. 80. По умолчанию, интернет-центр NBG334W выполняет функцию DHCP-сервера.
   - Если в вашей сети нет другого сервера DHCP, убедитесь, что IP-адреса компьютеров входят в ту же подсеть, что и NBG334W. См. Разд. 6.3 на с. 80.
5 Выполните сброс параметров устройства к заводским настройкам по умолчанию и попробуйте получить доступ к NBG334W с IP-адресом по умолчанию. См. Разд. 6.3 на с. 80.
6 Если неисправность не устраняется, обратитесь к сетевому администратору или поставщику оборудования, или выполните дополнительные рекомендации.

Дополнительные советы

- Попробуйте получить доступ к NBG334W с использованием другой службы, например, Telnet. Если доступ к NBG334W существует, проверьте параметры удаленного управления и правила межсетевого экрана, чтобы выяснить причину, по которой NBG334W не отвечает по HTTP.
- Если ваш компьютер не подключен к порту **WAN** или подключен по беспроводной связи, используйте компьютер, подключенный к порту **LAN/ETHERNET**.

Окно **Login (Вход в систему)** отображается, но невозможно выполнить вход в систему NBG334W.

1 Убедитесь, что пароль введен правильно. По умолчанию установлен пароль **1234**. Символы в это поле вводятся с учетом регистра, поэтому убедитесь, что клавиша [Caps Lock] выключена.
2 Нельзя получить доступ к Web-конфигуратору, если другой пользователь подключился к NBG334W через Telnet. Подключитесь к NBG334W позднее или попросите зарегистрированного пользователя выполнить выход из системы.
3 Отключите и снова подключите к NBG334W адаптер питания.
4 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 19.4 на с. 193.

Невозможно подключиться к NBG334W через Telnet.

См. рекомендации по поиску и устранению неисправностей в Не отображается окно Web-конфигуратора Login (Вход в систему) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

Невозможно выполнить загрузку/скачивание файла конфигурации с помощью FTP. / Не удается загрузить новую версию микропрограммы с помощью FTP.

См. рекомендации по поиску и устранению неисправностей в Не отображается окно Web-конфигуратора Login (Вход в систему) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

19.3 Доступ в Интернет

Невозможно получить доступ в Интернет.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство.
2. Проверьте, что введены правильно параметры учетной записи, предоставленные Интернет-провайдером. Символы в эти поля вводятся с учетом регистра, следовательно, проверьте, что [Caps Lock] выключен.
3. Если вы пытаетесь подключиться к сети Интернет по беспроводной связи, убедитесь, что клиентские настройки беспроводной совпадают с настройками в точке доступа.
4. Отключите все кабели от устройства и еще раз выполните инструкции Краткого руководства.
5. Если неисправность не устраняется, обратитесь к Интернет-Провайдеру.

Невозможно получить доступ в Интернет. Доступ в Интернет настроен через NBG334W, но подключение к Интернет больше не работает.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.4 на с. 15.
2. Перезагрузите NBG334W.
3. Если неисправность не устраняется, обратитесь к Интернет-Провайдеру.

Подключение к Интернет работает медленно или нестабильно.

1. Возможно, что локальная сеть перегружена. Посмотрите на светодиоды и проверьте их работу по Разд. 1.4 на с. 15. Если интернет-центр NBG334W посылает и передает большие объемы информации, закройте программы, которые используют Интернет, особенно равноправные приложения.
2. Проверьте уровень сигнала. Если сигнал слабый, переместите NBG334W ближе к точке доступа и обратите внимание на устройства, которые могут создавать помехи беспроводной сети (например, микроволновые печи, другие беспроводные сети и т.д.).
3. Перезагрузите NBG334W.
4. Если неисправность не устраняется, обратитесь к сетевому администратору или поставщику оборудования, или выполните дополнительные рекомендации.

Дополнительные советы

- Проверьте настройки управления полосой пропускания. Если управление отключено, попробуйте его включить. Если включено, попробуйте изменить распределение.
- Проверьте настройки качества обслуживания (QoS). Если управление отключено, попробуйте его включить. Если включено, можно попробовать повысить или понизить приоритет для некоторых приложений.

19.4 Восстановление заводских настроек NBG334W

При восстановлении заводских настроек NBG334W будут утеряны все сделанные изменения. При этом NBG334W перезагружает стандартные настройки и сбрасывает пароль на **1234**. Все настройки придется выполнять заново.

При нажатии на кнопку **RESET (СБРОС)** все внесенные изменения будут утеряны.

Порядок сброса настроек NBG334W:

1. Убедитесь, что светодиод **PWR** горит, не мигая.
2. Нажмите и удерживайте кнопку **RESET (СБРОС)** в течение пяти секунд. Отпустите кнопку **RESET**, когда светодиод **PWR** начнет мигать. Заводские настройки должны быть восстановлены.

Если интернет-центр NBG334W автоматически начнет перезагружаться, подождите окончания загрузки NBG334W и войдите в веб-конфигуратор. Используйте пароль «1234».

Если интернет-центр NBG334W не начнет автоматически перезагружаться, выключите и включите питание NBG334W. После этого следуйте вышеприведенным инструкциям.

19.5 Поиск и устранение неисправностей беспроводного маршрутизатора и точки доступа

? Нет доступа к NBG334W или устройство не может связаться ни с одним компьютером локальной беспроводной локальной сети (беспроводной точкой доступа или маршрутизатором).

1. Проверьте, что функция беспроводной сети включена на NBG334W
2. Убедитесь, что беспроводной адаптер беспроводной станции работает в нормальном режиме.
3. Убедитесь, что беспроводной адаптер, установленный на Вашем компьютере, имеет поддержку IEEE 802.11 и совместим с тем же беспроводным стандартом, который поддерживается в NBG334W.
4. Убедитесь, что Ваш компьютер (с установленным беспроводным адаптером) находится в зоне действия NBG334W.
5. Проверьте, что интернет-центр NBG334W и Ваша беспроводная станция имеют одинаковые настройки беспроводной сети и безопасности.
6. Убедитесь, что трафик между локальной и глобальной сетями не блокируется межсетевым экраном интернет-центра NBG334W.
7. Убедитесь, что к NBG334W разрешен удаленный доступ через интерфейс WLAN. Проверьте настройки удаленного доступа.

- Дополнительную информацию см. в руководстве пользователя в главе по беспроводной локальной сети.

19.6 Дополнительные функции

После входа в систему не отображаются некоторые окна и поля веб-конфигуратора.

Возможно, доступ к веб-конфигуратору происходит в основном режиме. Некоторые окна и поля доступны только в расширенном режиме. Выбрать нужный режим можно в окне **Maintenance (Сопровождение) > Config Mode (Режим настройки)**.

После блокирования URL по ключевому слову не пропал доступ к блокируемому веб-сайту.

Проверьте установку флажка **Enable URL Keyword Blocking (Включить блокирование URL по ключевым словам)** в окне **Content Filtering (Фильтрация содержимого)**. Убедитесь, что указанное ключевое слово присутствует в списке **Keyword List (Список ключевых слов)**.

Если ключевое слово содержится в списке **Keyword List**, но содержащие его URL-адреса не блокируются, настройте блокировку по ключевым словам с помощью команд. См. раздел «Настройка блокирования URL-адресов по ключевым словам» в главе «Фильтрация содержимого».

Часть VI
Приложения и алфавитный указатель

Характеристики и инструкция по настенному креплению (199)
Всплывающие окна, сценарии и разрешения Java (205)
IP-адреса и организация подсетей (211)
Настройка IP-адреса компьютера (221)
Беспроводные локальные сети (237)
Службы (251)
Сервисная служба (257)
Алфавитный указатель (263)

A

Характеристики и инструкция по настенному креплению

В следующей таблице представлены характеристики оборудования и программного обеспечения NBG334W.

Табл. 75 Аппаратные характеристики

Размеры (Ш Ч Г Ч В)	162 x 117 x 32 мм
Питание	~100-240 В, 50/60 Гц
Порты Ethernet	Автоматический выбор скорости: Функция автоматического выбора скорости позволяет интернет-центру NBG334W определять скорость входящей передачи и на основе этой информации производить настройку без стороннего вмешательства. Устройство поддерживает передачу данных на скорости 10 или 100 Мбит/с в полудуплексном или полнодуплексном режиме (в зависимости от режима сети Ethernet). Автоматический выбор кабеля: Допускает использование кабелей Ethernet, как с перекрестными (кроссовер), так и с прямыми соединениями.
4-портовый коммутатор	Интернет-центр NBG334W является выгодным и конкуренто-способным сетевым решением, благодаря комбинации функций коммутатора и маршрутизатора. К интернет-центру NBG334W можно подключить до четырех компьютеров, которые смогут выходить в Интернет через его порт WAN. Для этого не нужен концентратор. Количество компьютеров локальной сети можно увеличить с помощью концентратора.
Кнопка **Reset (Сброс)**	Данная кнопка находится на задней панели устройства. Она позволяет восстанавливать заводские настройки NBG334W. При нажатии на кнопку в течение 1 секунды произойдет перезагрузка устройства. При нажатии на кнопку в течение 5 секунд произойдет возврат к заводским настройкам.
Антенна	Интернет-центр NBG334W оборудовано съемной антенной чувствительностью 5 дБи (относительно изотопной антенны), обеспечивающей четкую радиопередачу и прием в беспроводной сети.
Рабочая температура	0є C ~ 50є C
Температура хранения	-20є C ~ 60є C
Рабочая влажность	20 ~ 95% относительной влажности (без конденсата)
Влажность при хранении	20 ~ 95% относительной влажности (без конденсата)

Табл. 75 Аппаратные характеристики

Расстояние между центрами отверстий на задней панели устройства	125 мм
Размер винтов для настенного крепления	M4

Табл. 76 Характеристики встроенного программного обеспечения

ФУНКЦИЯ	ОПИСАНИЕ
IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	1234
Диапазон DHCP	от 192.168.1.33 до 192.168.1.64
Управление устройством	Веб-конфигуратор упрощает настройку широкого спектра функций интернет-центра NBG334W.
Функции беспроводной связи	Интернет-центр NBG334W поддерживает беспроводное подключение клиентов по стандартам IEEE 802.11b и IEEE 802.11g. Клиенты стандарта IEEE 802.11g могут подключаться с использованием функции Super G. Для защиты беспроводной сети можно задействовать функции безопасности (WEP, WPA(2), WPA(2)-PSK) и фильтрацию на основе MAC-адресов. Примечание: NBG334W может воспринимать радиочастотные помехи от других устройств, работающих в диапазоне 2,4 ГГц, таких как микроволновые печи, радиотелефоны, устройства технологии Bluetooth и других беспроводных LAN.
Обновление микропрограммы	Загрузите новую версию микропрограммы (если есть) с Web-сайта ZyXEL и с помощью Web-конфигуратора, средства FTP или TFTP загрузите ее в интернет-центр NBG334W. Примечание: Необходимо загружать микропрограмму строго в соответствии с конкретной моделью устройства.
Резервное сохранение и восстановление конфигурации	Сделайте копию конфигурации интернет-центра NBG334W, которую можно будет в последующем загрузить обратно в NBG334W, если понадобится восстановить предыдущую конфигурацию.
Трансляция сетевых адресов (NAT)	Каждый компьютер в сети должен иметь уникальный IP-адрес. Используйте функцию NAT для преобразования общедоступного IP-адреса в несколько частных IP-адресов для компьютеров вашей сети.
Межсетевой экран	Чтобы обезопасить доступ в Интернет, на интернет-центре можно задействовать функцию межсетевого экрана. По умолчанию, когда межсетевой экран включен, весь входящий трафик из Интернет к локальной сети блокируется, если он не инициирован из этой локальной сети. Это значит, что внешнее зондирование вашей сети блокируется, но при этом Вы можете безопасно просматривать Интернет-сайты и загружать файлы.

Табл. 76 Характеристики встроенного программного обеспечения

ФУНКЦИЯ	ОПИСАНИЕ
Content Filter (Контент-фильтр)	Интернет-центр NBG334W блокирует или разрешает просмотр указанных веб-сайтов с URL, содержащими определенные ключевые слова. Можно указать периоды времени, в течение которых будет работать контент-фильтр. Кроме того, можно указать компьютеры, чей трафик следует фильтровать или, наоборот, не фильтровать. Помимо этого можно подписаться на фильтрацию по категориям, которая позволяет интернет-центру NBG334W проверять веб-сайты по внешней базе данных.
Управление пропускной способностью	Для определенных типов трафика и определенных компьютеров вашей сети можно зарезервировать полосу пропускания и задать им приоритет для повышения эффективности управления трафиком.
Время и дата	Можно синхронизировать текущее время и дату с внешним сервером времени при включении питания NBG334W. Время также можно установить вручную. Дата и время используются в регистрационных журналах.
Переадресация портов	Если в сети есть сервер (например, Web-сервер или сервер электронной почты), с помощью этой функции можно разрешить доступ к нему пользователям из Интернет.
DHCP (Протокол динамической настройки узла)	С помощью этой функции интернет-центр NBG334W назначает IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам локальной сети.
Поддержка динамической DNS	Поддержка динамической DNS (Domain Name System – система доменных имен) позволяет использовать фиксированный URL, например, www.zyxel.com с динамическим IP-адресом. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамической DNS.
Многоадресная рассылка IP	Многоадресная рассылка IP используется для отправки трафика определенной группе компьютеров. Интернет-центр NBG334W поддерживает версии 1 и 2 протокола IGMP (Internet Group Management Protocol – протокол управления группами в сети Интернет), который используется для присоединения к группам многоадресной рассылки (см. RFC 2236).
Псевдоним IP	Псевдоним IP позволяет разделить физическую сеть на логические подсети на одном интерфейсе Ethernet, при этом NBG334W действует как шлюз для каждой подсети.
Протоколирование и трассировка	Для диагностики неисправностей можно использовать пакетную трассирровку и журналы. Интернет-центр NBG334W позволяет отправлять журналы на внешний сервер UNIX, предназначенный для хранения системных журналов.
PPPoE	Протокол PPPoE имитирует коммутируемое подключение к сети Интернет через Ethernet-соединение.
Инкапсуляция PPTP	PPTP (Point-to-Point Tunneling Protocol – протокол туннелирования «точка - точка») обеспечивает безопасную передачу данных по сети VPN (Virtual Private Network – виртуальная частная сеть). Интернет-центр NBG334W поддерживает одно соединение PPTP одновременно.
Универсальная функция «Plug and Play» (UPnP)	Интернет-центр NBG334W может взаимодействовать с другими устройствами сети, поддерживающими UPnP.

Далее приводится не полный список стандартов, поддерживаемых интернет-центром NBG334W.

Табл. 77 Стандарты, поддерживаемые устройством

СТАНДАРТ	ОПИСАНИЕ
RFC 867	Протокол Daytime (дней)
RFC 868	Протокол Time (времени)
RFC 1112	IGMP v1 (межсетевой протокол управления группами)
RFC 1305	Протокол сетевого времени (NTP версии 3)
RFC 1631	Трансляция сетевых IP-адресов (NAT)
RFC 1661	Протокол соединения «точка - точка» (PPP)
RFC 2236	SNMPv2: Simple Network Management Protocol – Простой протокол управления сетью версии 2
RFC 2516	Метод передачи от точки к точке через сеть Интернет (PPPoE)
RFC 2766	Протокол трансляции сетевых адресов (NAT)
IEEE 802.11	Известный как Wi-Fi, он определяет набор стандартов беспроводной локальной или глобальной связи, определенный рабочей группой 11 комитета стандартизации IEEE LAN/MAN (IEEE 802).
IEEE 802.11b	Использует диапазон частот 2,4 гигагерц (ГГц)
IEEE 802.11g	Использует диапазон частот 2,4 гигагерц (ГГц)
IEEE 802.11d	Стандарты локальных сетей и сетей уровня города: мосты протокола управления доступом к среде передачи (MAC)
IEEE 802.11x	Контроль доступа в сеть через порты
IEEE 802.11e QoS	Стандарт беспроводной локальной связи IEEE 802.11 e для качества обслуживания
Microsoft PPTP	MS PPTP (протокол туннелирования между узлами в версии от Microsoft)

Инструкции по настенному монтажу

Для установки интернет-центра NBG334W на стену выполните следующее:

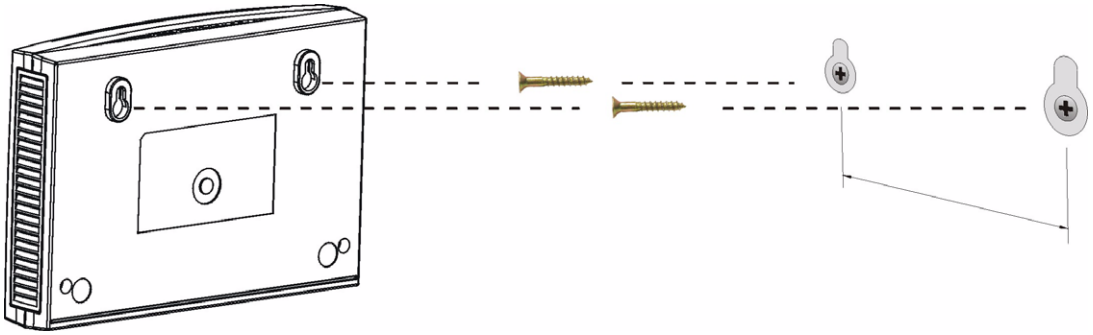
Посмотрите размер используемых саморезов и расстояние между центрами в Приложении «Технические характеристики изделия».

1. Найдите на стене свободное место, расположенное на достаточной высоте. Стена должна быть прочной.
2. Просверлите два отверстия под саморезы. Расстояние между центрами отверстий должно соответствовать указанному в приложении «Технические характеристики изделия».

При сверлении не повредите проходящие внутри стены трубы и скрытую проводку.

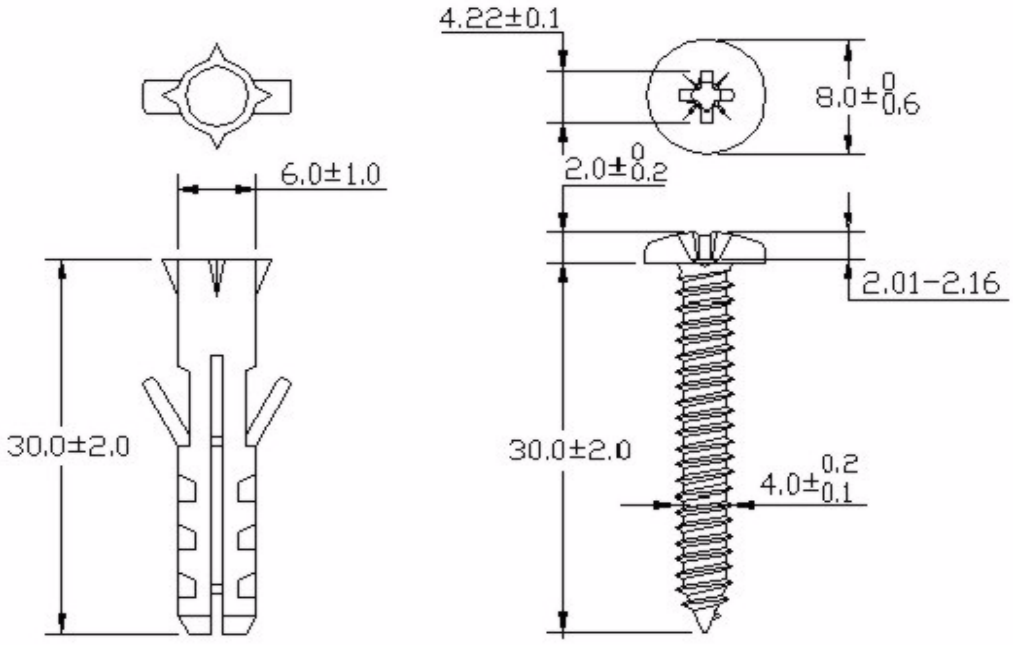
3. Не вкручивайте саморезы полностью. Оставьте небольшой зазор (около 5 мм) между головками саморезов и стеной.
4. Убедитесь, что саморезы надежно закреплены в стене. Они должны выдерживать вес интернет -центра NBG334W и соединительных проводов.
5. Совместите отверстия на задней панели интернет-центра NBG334W с саморезами в стене. Повесьте интернет-центр NBG334W на саморезы.

Рис. 93 Пример настенного монтажа



Далее указаны размеры винта M4 и дюбеля (используются для настенного монтажа). Все размеры даны в миллиметрах (мм).

Рис. 94 Дюбель и винт с резьбой M4



B

Всплывающие окна, сценарии и разрешения Java

Чтобы воспользоваться web-конфигуратором, необходимо включить следующие параметры:

- Инициированные модемом всплывающие окна в Интернет-браузере.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

В настоящем руководстве использованы снимки окон Internet Explorer 6. Окна в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

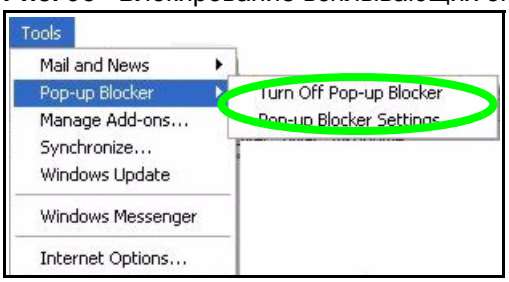
При регистрации пользователя устройства может возникнуть необходимость отключения блокирования всплывающих окон.

Либо отключите блокирование всплывающих окон (в Windows XP SP 2 оно по умолчанию включено), либо разрешите его и создайте исключение для IP-адреса Вашего устройства.

Отключение блокирования всплывающих окон

1 Откройте Internet Explorer, выберите **Tools (Сервис)**, **Pop-up Blocker (Блокирование всплывающих окон)**, затем **Turn Off Pop-up Blocker (Выключить блокирование всплывающих окон)**.

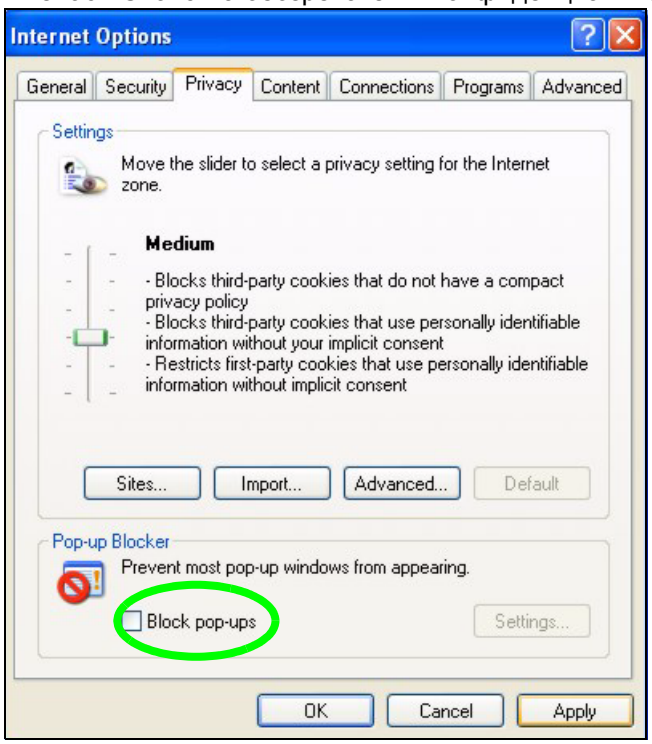
Рис. 95 Блокирование всплывающих окон



Вы также можете проверить, отключено ли блокирование всплывающих окон в разделе **Pop-up Blocker (Блокирование всплывающих окон)** на вкладке **Privacy (Конфиденциальность)**.

1. Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Снимите флажок **Block pop-ups (Блокировать всплывающие окна)** в разделе **Pop-up Blocker (Блокирование всплывающих окон)** в нижней части окна. Это отключит блокирование всплывающих окон.

Рис. 96 Свойства обозревателя: Конфиденциальность



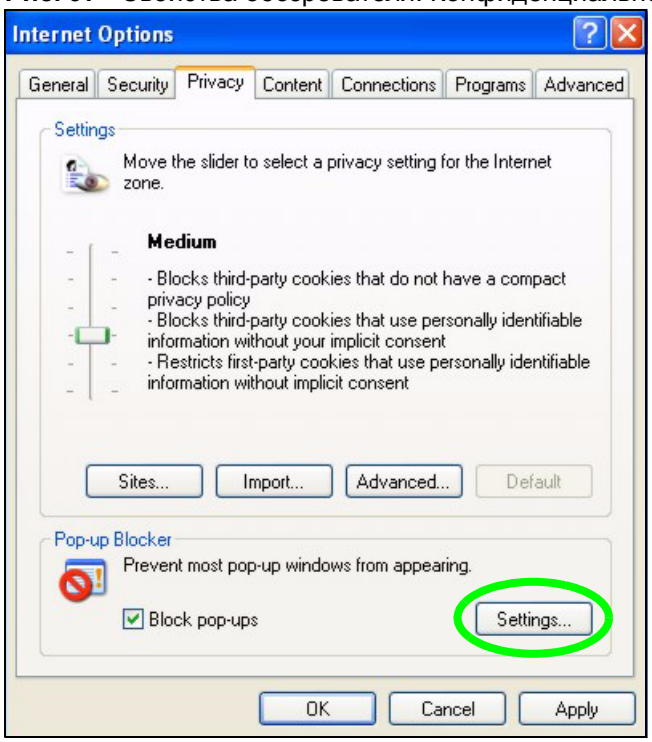
3. Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки.

Включение блокировки всплывающих окон с исключениями

Если же Вы хотите, чтобы всплывающие окна были разрешены лишь на Вашем устройстве, то можно сделать следующее.

1. Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Выберите **Settings… (Параметры...)** – откроется окно **Pop-up Blocker Settings (Параметры блокирования всплывающих окон)**.

Рис. 97 Свойства обозревателя: Конфиденциальность



3 Введите IP-адрес Вашего устройства (web-сайт, который Вы не хотите блокировать) с префиксом «http://». Например, введите http://192.168.167.1.

4 Нажмите кнопку **Add (Добавить)** для переноса IP-адреса в список **Allowed sites (Разрешенные веб-узлы)**.

Рис. 98 Параметры блокирования всплывающих окон

5 Для возврата на вкладку **Privacy (Конфиденциальность)** нажмите кнопку **Close (Закрыть)**.

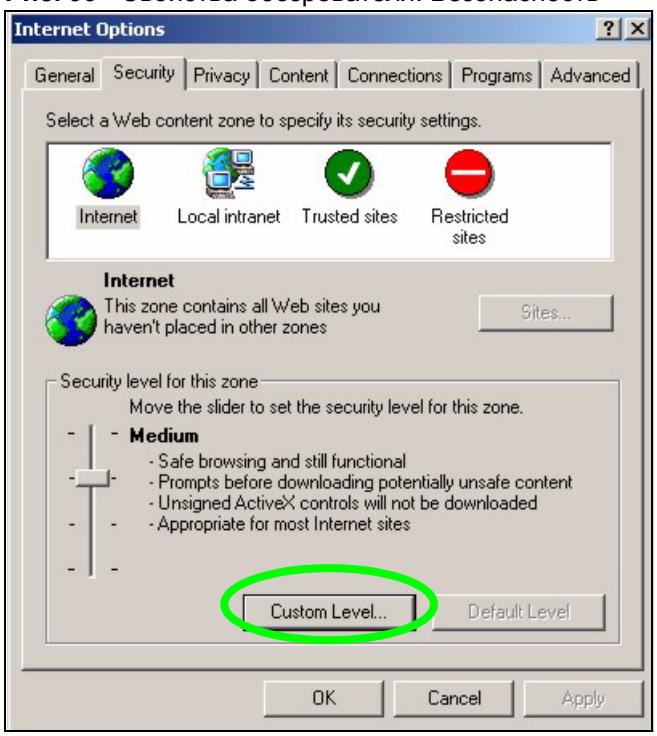
6 Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки.

Сценарии Java (JavaScripts)

Если страницы web-конфигуратора отображаются в Internet Explorer некорректно, проверьте, разрешено ли использование сценариев Java.

1 Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и закладку **Security (Безопасность)**.

Рис. 99 Свойства обозревателя: Безопасность



2 Нажмите кнопку **Custom Level... (Другой...)**.

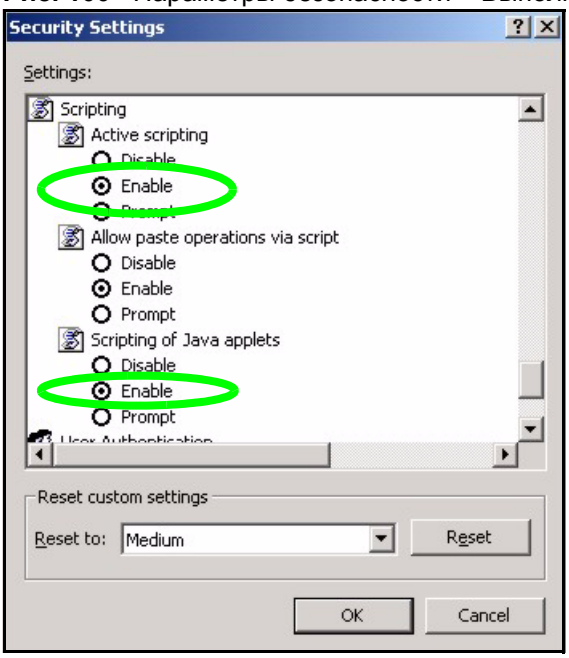
3 Пролистайте до раздела **Scripting (Сценарии)**.

4 В разделе **Active scripting (Активные сценарии)** должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

5 В разделе **Scripting of Java applets (Выполнять сценарии приложений Java)** также должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

6 Нажмите кнопку **OK**, чтобы закрыть окно.

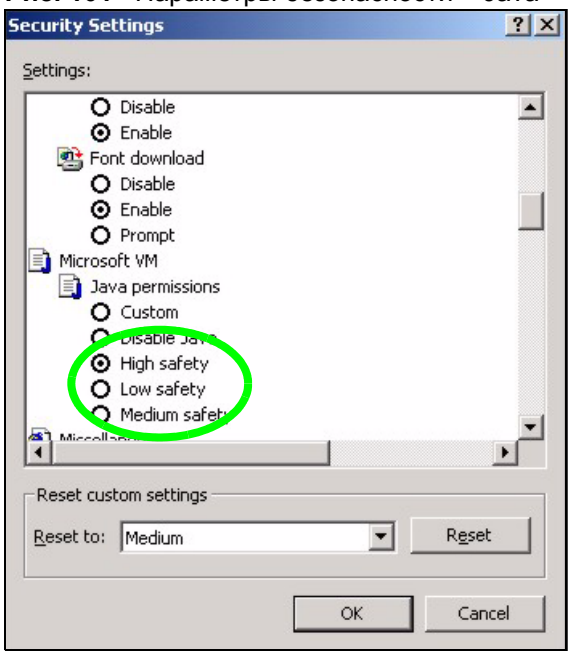
Рис. 100 Параметры безопасности – Выполнение сценариев приложений Java



Разрешения Java

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и затем закладку **Security (Безопасность)**.
2. Нажмите кнопку **Custom Level... (Другой...)**.
3. Спуститесь вниз к разделу **Microsoft VM**.
4. В разделе **Java permissions (Разрешения Java)** выберите уровень безопасности.
5. Нажмите кнопку **OK**, чтобы закрыть окно.

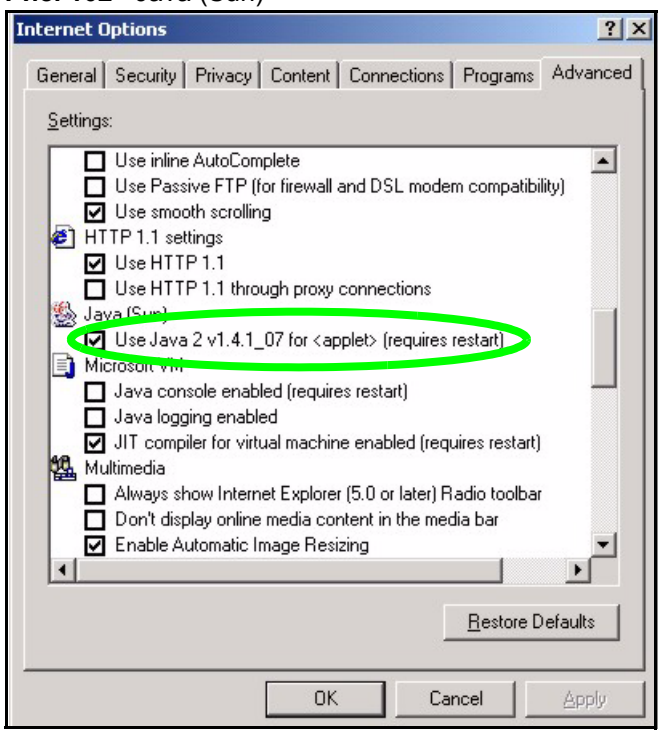
Рис. 101 Параметры безопасности – Java



JAVA (Sun)

1. Откройте Internet Explorer, выберите **Tools (Сервис), Internet Options (Свойства обозревателя), Advanced (Дополнительно)**.
2. Убедитесь, в разделе **Java (Sun)** установлено **Use Java 2 for <applet> (Использовать Java 2 для приложения)**.
3. Нажмите кнопку **OK**, чтобы закрыть окно.

Рис. 102 Java (Sun)



C

IP-адреса и организация подсетей

В этом приложении представлена информация об IP-адресах и масках подсети.

IP-адрес определяет конкретное устройство в сети. Каждому сетевому устройству (включая компьютеры, серверы, маршрутизаторы, принтеры и т.д.) для обмена информацией по сети требуется IP-адрес. Такие сетевые устройства также называют узлами.

Маска подсети определяет максимальное количество узлов в сети. Также маски подсети используются для разделения сети на несколько подсетей.

Описание IP-адресов

Одна часть IP-адреса является номером сети, а другая часть – номером узла. Так же, как все дома, находящиеся на одной улице, имеют общее название улицы, все узлы в локальной сети имеют общий номер сети. Так же, как каждый дом имеет индивидуальный номер, каждый узел в сети имеет уникальный идентификационный номер – идентификатор узла.Номер сети используется маршрутизаторами при отправке пакетов в соответствующую сеть, а идентификатор узла определяет конкретное устройство в этой сети для доставки этих пакетов.

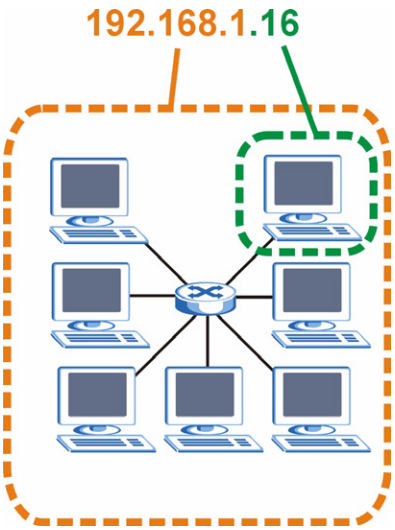
Структура

IP-адрес состоит их четырех частей, записанных в десятичном виде с разделительными точками, например: 192.168.1.1. Каждая из четырех частей называется байтом. Байт – это восьмизначное двоичное число (например, число 11000000 в десятичном представлении равно 192).

Следовательно, каждый байт имеет диапазон возможных значений от 00000000 до 11111111 в двоичном формате, или от 0 до 255 в десятичном.

На следующем рисунке показан пример IP-адреса, в котором три первых байта (192.168.1) являются номером сети, а четвертый байт (16) является идентификатором узла.

Рис. 103 Номер сети и идентификатор узла



Какая часть IP-адреса является номером сети и как идентификатор узла меняется в соответствии с маской подсети.

Маска подсети

С помощью маски подсети можно определить, какие биты являются частью номера сети, а какие – частью идентификатора узла (используя операцию логического «И»). Термин “подсеть” это сокращенное название для “физически независимого сегмента сети”.

Маска подсети состоит из 32 битов. Если бит маски подсети имеет значение 1, это значит, что соответствующий бит IP-адреса является частью номера сети. Если бит маски подсети имеет значение 0, это значит, что соответствующий бит IP-адреса является частью идентификатора узла.

В следующем примере показаны маска подсети, определяющая номер сети (жирным шрифтом), и идентификатор узла для IP-адреса 192.168.1.2.

Табл. 78 Маска подсети – указывает номер сети

	1-Й БАЙТ: (192)	**2-Й БАЙТ: (168)**	**3-Й БАЙТ: (1)**	**4-Й БАЙТ: (2)**
IP-адрес (в двоичной форме)	11000000	10101000	00000001	00000010
Маска подсети (в двоичной форме)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор узла				00000010

По договоренности маска подсети всегда состоит из непрерывной последовательности единиц в начале маски (слева), за которой следует непрерывная последовательность нулей общей длиной в 32 бита.

Маски подсети определяют какую часть в адресе составляет номер сети (т.е. биты со значением “1”). Например, “8-битная маска” означает, что первые 8 битов маски являются единицами, а оставшиеся 24 бита – нулями.

Маски подсети записываются в десятичном виде с разделительными точками, так же, как и IP-адреса. В следующем примере показаны 8-битные, 16-битные, 24-битные и 29-бит маски подсети в двоичном и десятичном виде.

Табл. 79 Маска подсети

	ДВОИЧНАЯ ФОРМА				В ДЕСЯТИЧНОМ ВИДЕ
	1-Й БАЙТ:	2-Й БАЙТ:	3-Й БАЙТ:	4-Й БАЙТ:	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Размер сети определяет максимально возможное число узлов, которое может находиться в сети. Чем больше число битов в номере сети, тем меньше число битов, остающихся для идентификатора узла.

IP-адрес, в котором идентификатор узла состоит только из нулей, является IP-адресом сети (например, 192.168.1.0 с 24-битной маской подсети). IP-адрес, в котором идентификатор узла состоит только из единиц, является широковещательным адресом для этой сети (например, 192.168.1.255 с 24-битной маской подсети).

Поскольку эти два IP-адреса нельзя использовать для отдельных узлов, максимально возможное число узлов в сети рассчитывается следующим образом:

Табл. 80 Максимальное число узлов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА УЗЛА В АДРЕСЕ		МАКСИМАЛЬНОЕ ЧИСЛО УЗЛОВ
8 бита	255.0.0.0	24 бита	$2^{24} – 2$	16777214
16 бита	255.255.0.0	16 бита	$2^{16} – 2$	65534
24 бита	255.255.255.0	8 бита	$2^{8} – 2$	254
29 бита	255.255.255.248	3 бита	$2^{3} – 2$	6

Записи маски подсети

Поскольку маска всегда состоит из непрерывной последовательности единиц в начале и непрерывной последовательности нулей в оставшихся битах и имеет длину 32 бита, можно просто указывать количество единиц вместо того, чтобы записывать значение каждого байта. Это обычно обозначается путем записи после адреса символа «/» и количества бит с единицами.

Например, запись 192.1.1.0 /25 равносильна записи 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице показаны несколько масок подсети с использованием обоих видов записи.

Табл. 81 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНАЯ ЗАПИСЬ	ПОСЛЕДНИЙ БАЙТ (В ДВОИЧНОЙ ФОРМЕ)	ПОСЛЕДНИЙ БАЙТ (В ДЕСЯТИЧНОЙ ФОРМЕ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

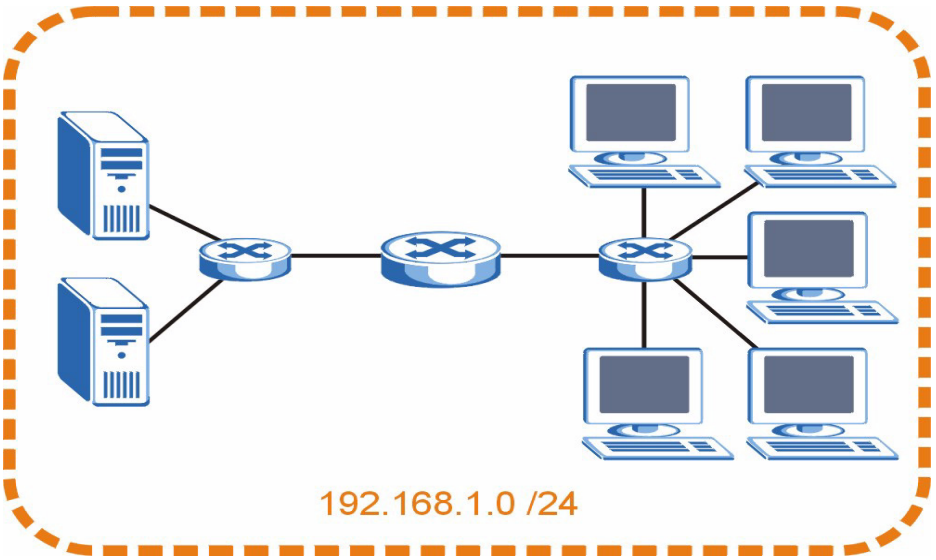
Организация подсетей

Маски подсети также используются для разделения сети на несколько подсетей.
В следующем примере сетевой администратор создал 2 подсети, чтобы изолировать группу серверов от остальной сети компании в целях безопасности.

В этом примере адрес сети компании – 192.168.1.0. Первые 3 байта адреса (192.168.1) являются номером сети, а оставшийся байт является идентификатором узла, следовательно, максимальное число узлов в этой сети равно $2^8 – 2$ или 254.

На следующем рисунке показана сеть компании до разделения на подсети.

Рис. 104 Пример организации подсетей: до разделения на подсети

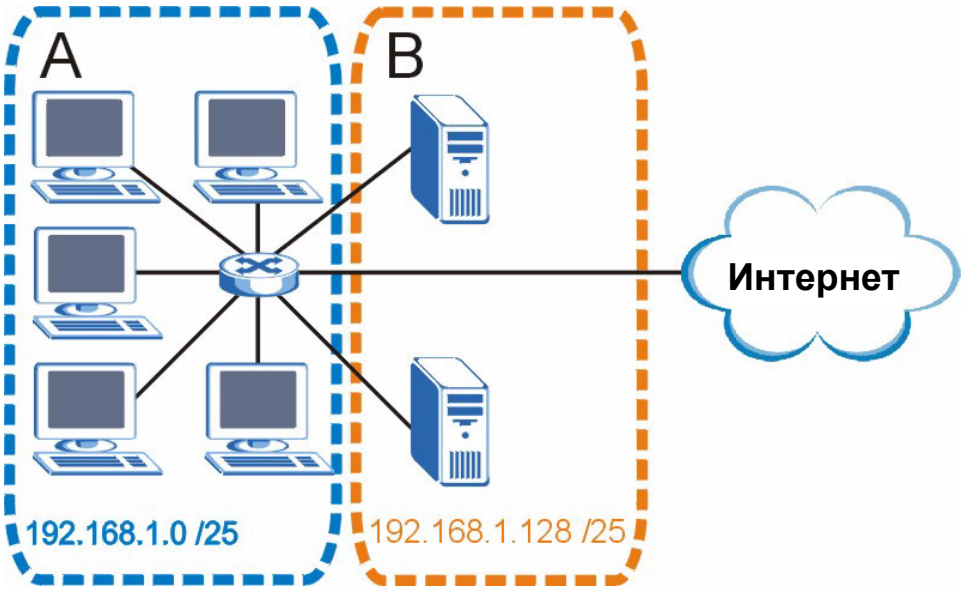


Можно «занять» один бит идентификатора узла для разделения сети 192.168.1.0 на две отдельные подсети. Маска подсети состоит теперь из 25 битов (255.255.255.128 или /25).

«Заимствованный» бит идентификатора узла может принимать значения 0 или 1, давая, таким образом, две подсети; 192.168.1.0 /25 и 192.168.1.128 /25.

На следующем рисунке показана сеть компании после разделения на подсети. Теперь организовано две подсети, **A** и **B**.

Рис. 105 Пример организации подсетей: после разделения на подсети



При 25-битной маске подсети в идентификаторе узла остается 7 битов, следовательно, максимальное число узлов в каждой подсети равно $2^7 - 2$ или 126 (идентификатор узла, состоящий только из нулей является адресом самой подсети, а состоящий только из единиц – широковещательным адресом этой подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 определяет подсеть **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для подсети **A** – 192.168.1.1, а старший – 192.168.1.126.

Подобным образом рассчитывается диапазон идентификаторов узлов для подсети **B**: от 192.168.1.129 до 192.168.1.254.

Пример: Четыре подсети

В предыдущем примере продемонстрировано использование 25-битной маски подсети для разделения 24-битного адреса на две подсети. Аналогично для разделения 24-битного адреса на четыре подсети, потребуется «заимствовать» два бита из идентификатора узла для получения четырех возможных комбинаций: 00, 01, 10 и 11. Маска подсети имеет 26 бит (11111111.11111111.11111111.**11**000000) или 255.255.255.192.

Каждая подсеть имеет 6 битов для идентификатора узла, при этом получается $2^6 – 2$ или 62 узла в каждой подсети (все нули в индентификаторе узла обозначают саму подсеть, все единицы являются широковещательным адресом этой подсети).

Табл. 82 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес (в десятичной форме)	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**00**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.0	Минимальный идентификатор узла: 192.168.1.1	
Адрес широковещательной рассылки: 192.168.1.63	Максимальный идентификатор узла: 192.168.1.62	

Табл. 83 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	64
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**01**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.64	Минимальный идентификатор узла: 192.168.1.65	
Адрес широковещательной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 84 Подсеть 3

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**10**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.128	Минимальный идентификатор узла: 192.168.1.129	
Адрес широковещательной рассылки: 192.168.1.191	Максимальный идентификатор узла: 192.168.1.190	

Табл. 85 Подсеть 4

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	192
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**11**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.192	Минимальный идентификатор узла: 192.168.1.193	
Адрес широковещательной рассылки: 192.168.1.255	Максимальный идентификатор узла: 192.168.1.254	

Пример: Восемь подсетей

Аналогично используется 27-битная маска для создания 8 подсетей (000, 001, 010, 011, 100, 101110111).

В следующей таблице приведены значения битов последнего байта IP-адреса для каждой подсети.

Табл. 86 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Проектирование подсетей

В следующей таблице представлена сводка для проектирования подсетей в сети с 24-битным номером сети.

Табл. 87 Проектирование подсетей в сети с 24-битным номером сети

КОЛИЧЕСТВО «ЗАИМСТВОВАННЫХ» БИТОВ УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

В следующей таблице представлена сводка для проектирования подсетей в сети с 16-битным номером сети.

Табл. 88 Проектирование подсетей в сети с 16-битным номером сети

КОЛИЧЕСТВО «ЗАИМСТВОВАННЫХ» БИТОВ УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Настройка IP-адресов

Номер сети зависит от конкретной ситуации. Если поставщик Интернет-услуг или сетевой администратор назначают блок зарегистрированных IP-адресов, то необходимо руководствоваться их указаниями при выборе IP-адреса и маски подсети.

Если поставщик Интернет-услуг не предоставляет явным образом адрес сети, то, скорее всего, вы используете учетную запись одиночного пользователя, и поставщик Интернет-услуг будет назначать динамический IP-адрес при каждом установлении соединения. В этом случае рекомендуется установить IP-адрес в диапазоне от 192.168.0.0 до 192.168.255.0. Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало этот диапазон специально для частного использования. Если явно не предписано использовать другие адреса, не следует использовать номера за пределами этого диапазона. Необходимо также включить функцию «NAT» (Network Address Translation – трансляция сетевых адресов) в NBG334W.

Выбрав номер сети, выберите для NBG334W IP-адрес, который легко запоминается, например, 192.168.1.1, но убедитесь, что никакое другое устройство в вашей сети не использует этот IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. NBG334W автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную NBG334W, без прямых указаний.

IP-адреса для частных сетей

Каждый компьютер в сети Интернет должен иметь уникальный адрес. Если сеть изолирована от Интернет, например, соединяет между собой локальные сети двух филиалов, можно без проблем назначать узлам произвольные IP-адреса. Тем не менее, агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало следующие три блока IP-адресов специально для частных сетей:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

IP-адрес может быть получен от IANA, от поставщика Интернет-услуг или может быть назначен частной сетью. Если ваша организация относительно небольшая, и доступ в Интернет осуществляется через поставщика Интернет-услуг, поставщик Интернет-услуг может предоставить адреса Интернет для ваших локальных сетей. С другой стороны, если организация является частью большой компании, следует проконсультироваться с сетевым администратором по поводу назначения IP-адресов.

Независимо от конкретной ситуации не стоит назначать произвольные IP-адреса; лучше следовать приведенным выше указаниям. Для получения более подробной информации по назначению адресов см. RFC 1597, *Address Allocation for Private Internets (Назначение адресов в частных сетях)* и RFC 1466, *Guidelines for Management of IP Address Space (Руководство по управлению пространством IP-адресов)*.

D

Настройка IP-адреса компьютера

На всех компьютерах должны быть установлены сетевые платы Ethernet 10 или 100 Мбит/с и протоколы TCP/IP.

Операционные системы Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и выше, а также все версии систем UNIX/LINUX уже содержат программные компоненты, необходимые для инсталляции и использования стека протоколов TCP/IP. При использовании ОС Windows 3.1 необходимо приобрести пакет прикладных программ TCP/IP от стороннего производителя.

На компьютерах с операционными системами Windows NT/2000/XP, Macintosh OS 7 (или более поздними) компоненты TCP/IP должны быть уже установлены.

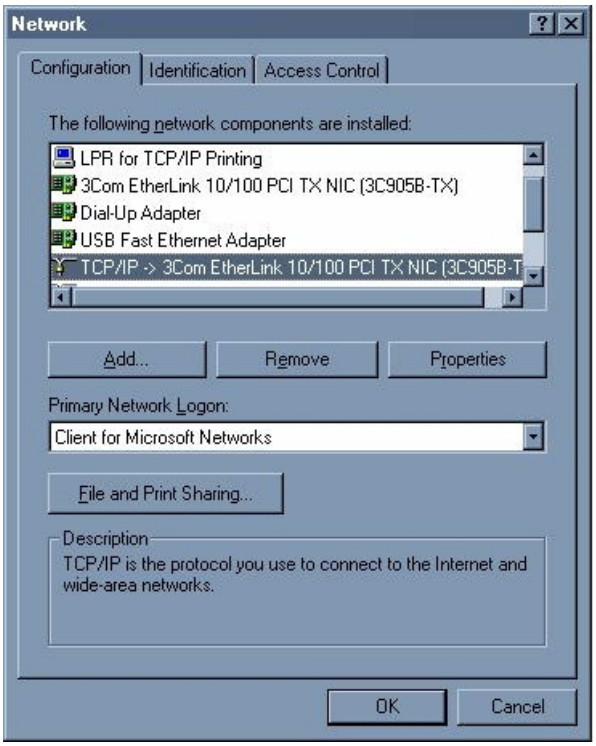
После установки компонентов TCP/IP, настройте параметры TCP/IP для соединения с сетью.

Если параметры IP назначаются вручную вместо динамического назначения, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN интернет-центра.

Windows 95/98/Me

Нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните по значку **Network (Сеть)**, чтобы открыть окно **Network**.

Рис. 106 WIndows 95/98/Me: Сеть: Конфигурация



Установка компонентов

В окне **Network (Сеть)** на закладке **Configuration (Конфигурация)** отображается список установленных компонентов. Вам потребуется сетевая карта, протокол TCP/IP и клиент для сетей Microsoft.

Если необходимо установить сетевую плату:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Adapter (Сетевая плата)** и нажмите **Add (Добавить)**.
3. Выберите производителя и модель вашей сетевой платы и нажмите **OK**.

Если необходимо установить протокол TCP/IP:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Protocol (Протокол)** и нажмите **Add (Добавить)**.
3. Выберите «**Microsoft**» из списка **manufacturers (производители)**.
4. Выберите **TCP/IP** из списка сетевых протоколов и нажмите кнопку **OK**.

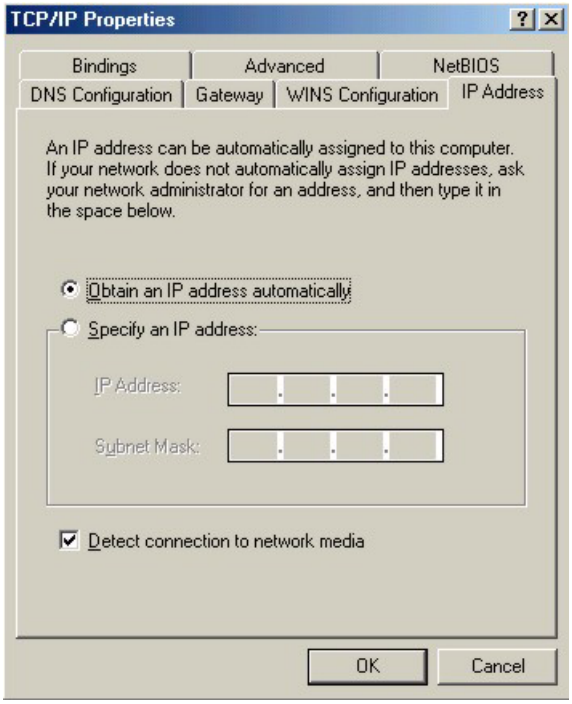
Если необходимо установить Клиента для сетей Microsoft:

1. Нажмите кнопку **Add** (**Добавить)**.
2. Выберите **Client (Клиент)** и нажмите кнопку **Add (Добавить)**.
3. Выберите **«Microsoft»** из списка производителей.
4. Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** из списка сетевых клиентов и нажмите кнопку **OK**.
5. Перезагрузите компьютер, чтобы произведенные изменения вступили в силу.

Настройка

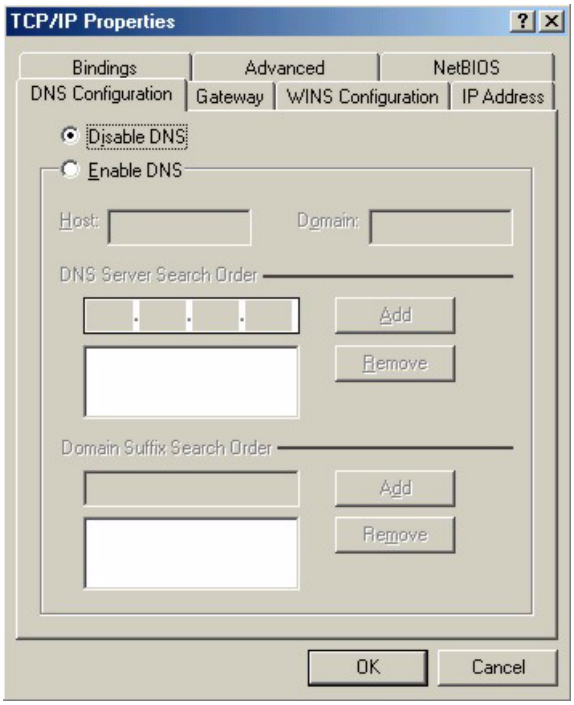
1. В окне **Network (Сеть)** выберите закладку **Configuration (Конфигурация)**, выберите пункт TCP/IP для вашей сетевой платы и нажмите **Properties (Свойства)**.
2. Выберите закладку **IP-адрес**.
   - Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
   - Если вы используете статический IP-адрес, выберите вариант **Specify an IP address (Указать IP-адрес явным образом)** и заполните поля **IP address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

Рис. 107 Windows 95/98/Me: Свойства протокола TCP/IP: IP-адрес



3. Выберите закладку **DNS Configuration (Конфигурация DNS)**.
   - Если вы не знаете параметры DNS, выберите **Disable DNS (Отключить DNS)**.
   - Если вам известны параметры DNS, выберите **Enable DNS (Включить DNS)** и заполните поля, расположенные ниже (возможно, потребуется заполнять не все поля).

Рис. 108 Windows 95/98/Me: Свойства протокола TCP/IP: Конфигурация DNS



4 Выберите закладку **Gateway (Шлюз)**.
   - Если вы не знаете IP-адрес шлюза, удалите все установленные ранее шлюзы.
   - Если у вас есть IP-адрес шлюза, введите его в поле **New gateway (Новый шлюз)** и нажмите кнопку **Add (Добавить)**.
5 Нажмите **OK**, чтобы сохранить сделанные изменения и закрыть окно **TCP/IP Properties (Свойства: TCP/IP)**.
6 Нажмите кнопку **OK**, чтобы закрыть окно **Network (Сеть)**. При появлении запроса вставьте в дисковод компакт-диск Windows.
7 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка настроек

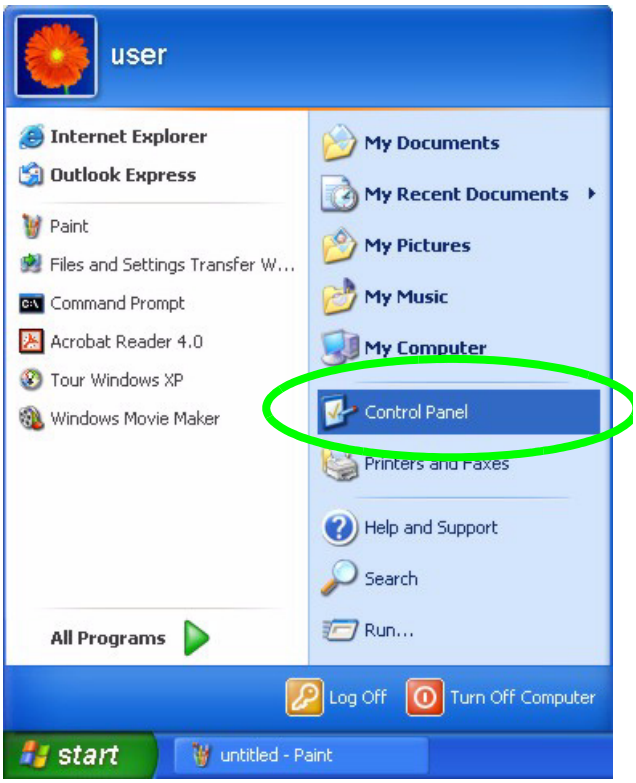
1 Нажмите кнопку **Start (Пуск)**, а затем выберите пункт **Run (Выполнить)**.
2 В окне **Run (Выполнить)** введите команду «winipcfg», а затем нажмите **OK** для отображения окна **IP Configuration (Конфигурация IP)**.
3 Выберите свой сетевой адаптер. При этом должны отображаться IP-адрес и маска подсети вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

В следующих рисунках используется тема графического интерфейса Windows XP по умолчанию.

1 Нажмите **start (пуск)** (**Start (Пуск)** в Windows 2000/NT), **Settings (Настройка)**, **Control Panel (Панель управления)**.

Рис. 109 Windows XP: Меню Пуск

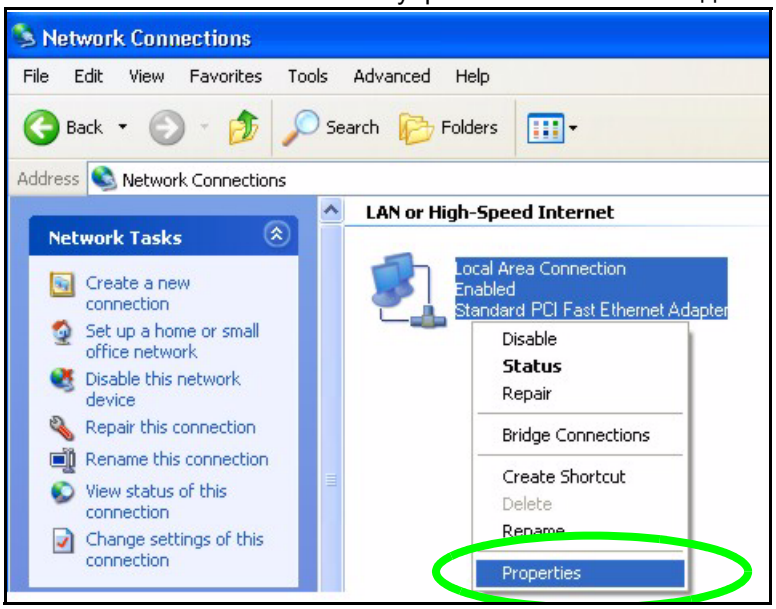


2 На **Панели управления** дважды щелкните **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

Рис. 110 Windows XP: Control Panel (Windows XP: Панель управления)

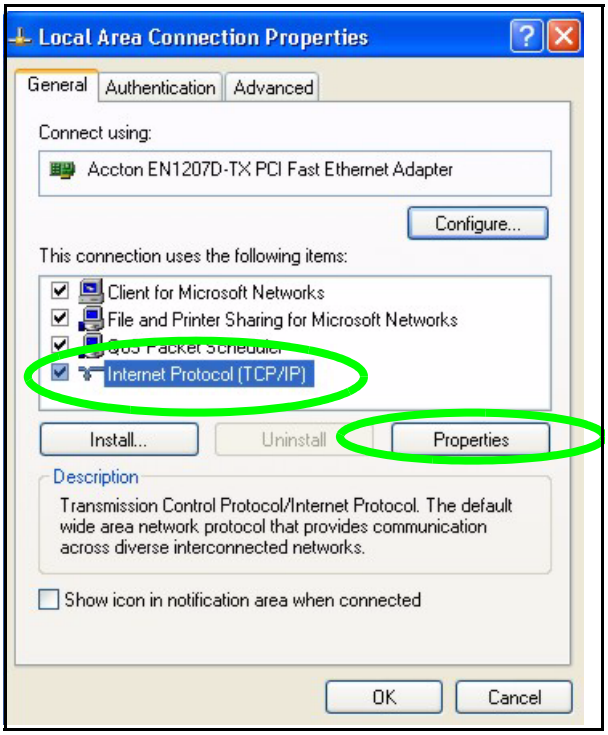
3 Щелкните правой кнопкой мыши значок **Local Area Connection (Подключение по локальной сети)** и выберите **Properties (Свойства)**.

Рис. 111 Windows XP: Панель управления: Сетевые подключения: Свойства



4 На вкладке **General (Общие)** в WinXP выберите **Internet Protocol (TCP/IP)** (Протокол Интернета (TCP/IP)) и нажмите **Properties (Свойства)**.

Рис. 112 Windows XP: Подключение по локальной сети: Свойства

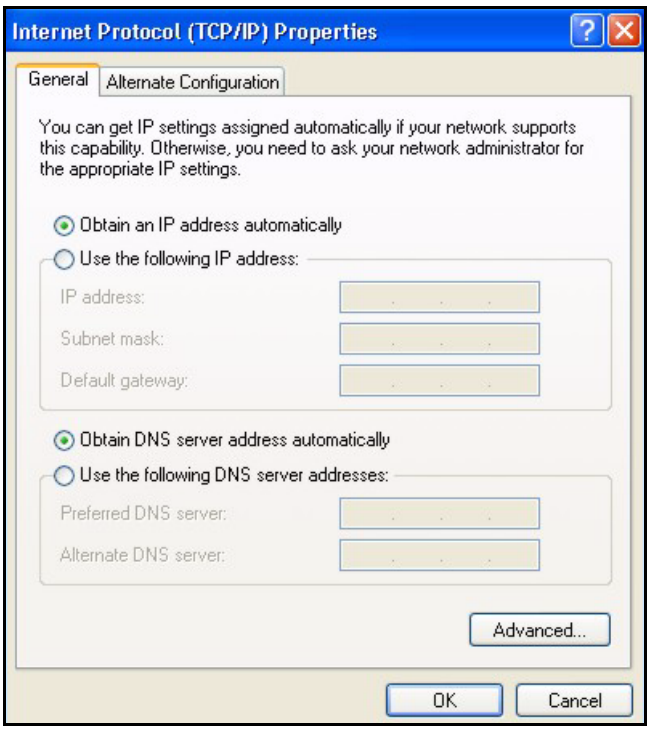


5 Откроется окно **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** (закладка **General (Общие)** в Windows XP).

- Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

- Если вы имеете статический IP-адрес, выберите **Use the following IP Address (Использовать следующий IP-адрес)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Основной шлюз)**.
- Нажмите кнопку **Advanced (Дополнительно)**.

Рис. 113 Windows XP: Свойства: Протокол Интернета (TCP/IP)



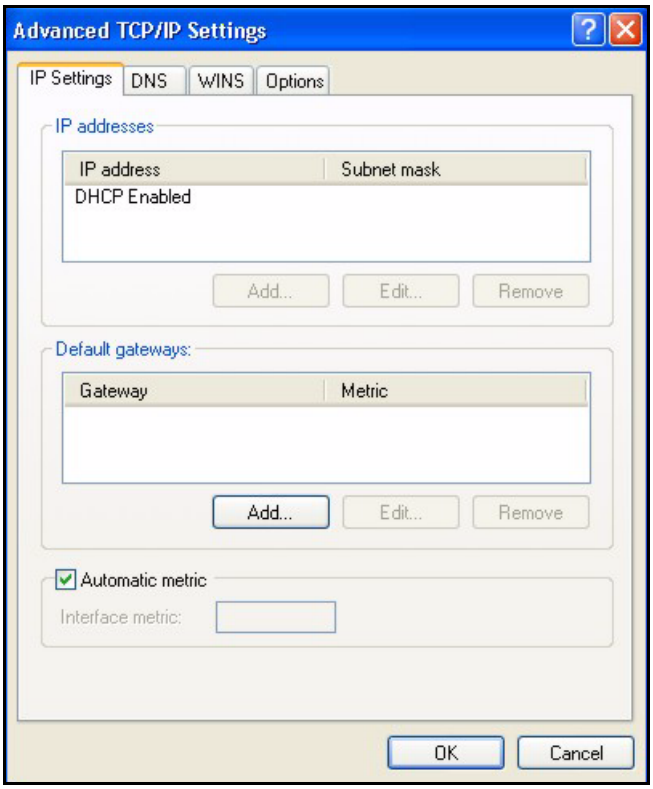
6 Если Вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке **IP Settings (Параметры IP)** и нажмите **OK**.

Для настройки дополнительных IP-адресов выполните следующие действия:

- На закладке **IP Settings (Параметры IP)** в поле для IP-адресов нажмите **Add (Добавить)**.
- В окне **TCP/IP Address (Адрес TCP/IP)** введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем нажмите кнопку **Add (Добавить)**.
- Повторите описанные выше действия для каждого IP-адреса, который необходимо добавить.
- Настройте дополнительные основные шлюзы на закладке **IP Settings (Параметры IP)**, щелкнув по кнопке **Add (Добавить)** в разделе **Default gateways (Основные шлюзы)**.
- В окне **TCP/IP Gateway Address (Адрес шлюза TCP/IP)**, введите IP-адрес шлюза по умолчанию в поле **Gateway (Шлюз)**. Для ручной настройки метрики по умолчанию (количества транзитных пунктов при передаче), снимите флажок **Automatic metric (Автоматическая метрика)** и введите значение в поле **Metric (Метрика)**.
- Нажмите кнопку **Add (Добавить)**.

- Повторите предыдущие три действия для всех шлюзов, которые необходимо добавить.
- По завершении настройки нажмите кнопку **OK**.

Рис. 114 Windows XP: Дополнительные свойства TCP/IP

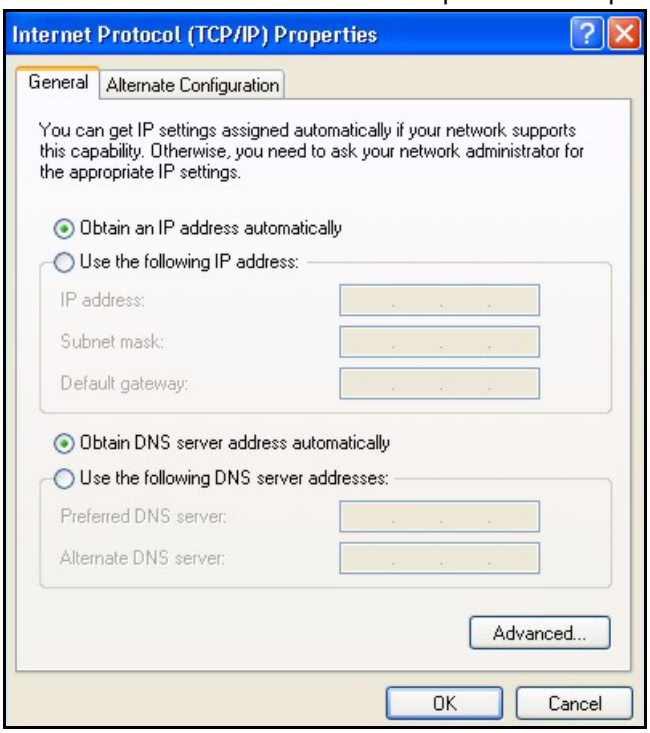


7 В окне **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** на закладке **General (Общие)** в Windows XP:

- Выберите **Obtain DNS server automatically (Получить адрес DNS-сервера автоматически)**, если вы не знаете IP-адрес(а) сервера(ов) DNS.
- Если вы знаете IP-адрес(а) сервера(ов) DNS, выберите **Use the following DNS server addresses (Использовать следующие адреса серверов DNS)**, и введите адреса в поля **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.

  Если серверы DNS были настроены ранее, нажмите **Advanced (Дополнительно)** и затем закладку **DNS** для определения порядка их использования.

Рис. 115 Windows XP: Свойства: Протокол Интернета (TCP/IP)



8 Нажмите **OK**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета (TCP/IP))**.

9 Нажмите кнопку **Close (Закрыть)** (**OK** в Windows 2000/NT), чтобы закрыть окно **Local Area Connection Properties (Свойства подключения по локальной сети)**.

10 Закройте окно **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

11 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка настроек

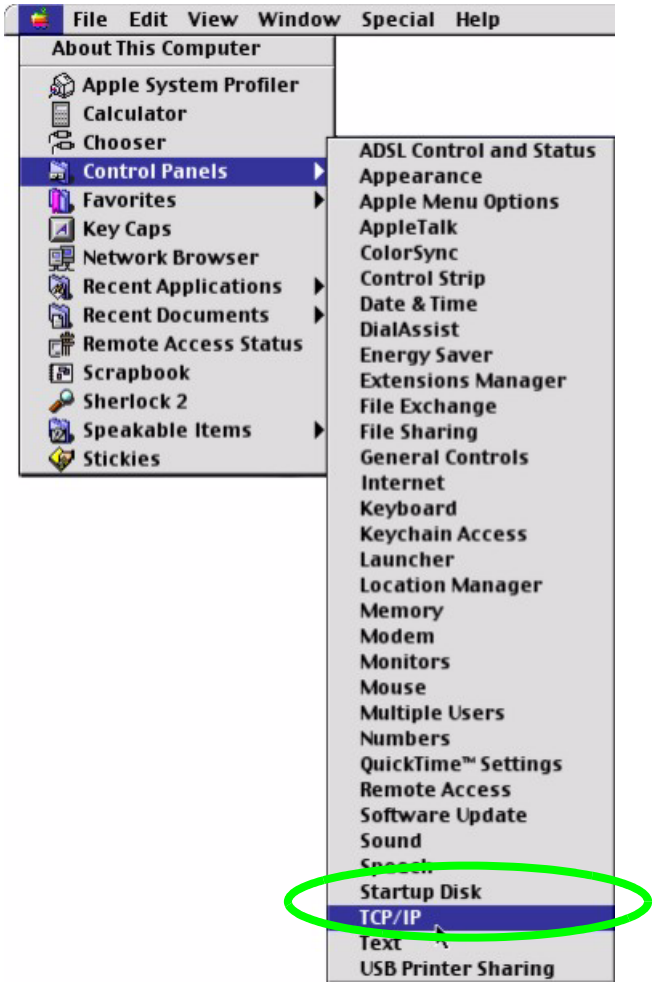
1 Щелкните **Start (Пуск), All Programs (Все программы), Accessories (Стандартные)**, а затем **Command Prompt (Командная строка)**.

2 В окне **Command Prompt (Командная строка)** введите команду «ipconfig» и нажмите клавишу [ENTER]. Также можно открыть окно **Network Connections (Сетевые подключения)**, щелкнуть правой кнопкой мыши на сетевом подключении, выбрать **Status (Состояние)** и затем щелкнуть закладку **Support (Поддержка)**.

Macintosh OS 8/9

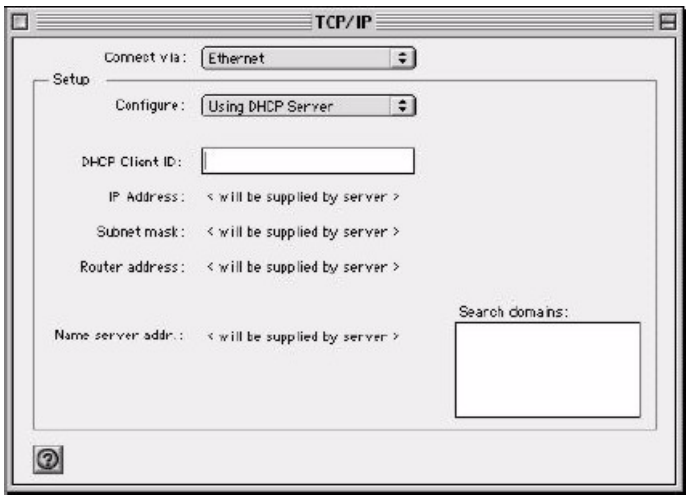
1 Нажмите кнопку меню **Apple**, выберите **Control Panel (Панель управления)**, а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 116 Macintosh OS 8/9: Меню Apple



2 Выберите **Ethernet built-in (Встроенный сетевой контроллер)** из списка **Connect via (Подключение через...)**.

Рис. 117 Macintosh OS 8/9: TCP/IP



3 Для настройки динамических параметров выберите **Using DHCP (Использовать сервер DHCP)** в списке **Configure: (Настроить)**.

4 Для настройки статических параметров выполните следующие действия:
   - В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
   - Введите IP-адрес в окне **IP Address (IP-адрес)**.
   - Введите маску подсети в окне **Subnet mask (Маска подсети)**.
   - Введите IP-адрес интернет-центра в поле **Router address (Адрес маршрутизатора)**.
5 Закройте окно **TCP/IP Control Panel (Панель управления TCP/IP)**.
6 При появлении запроса нажмите **Save (Сохранить)** для сохранения изменений в конфигурации.
7 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

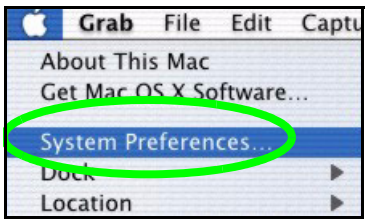
Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel (Панель управления TCP/IP)**.

Macintosh OS X

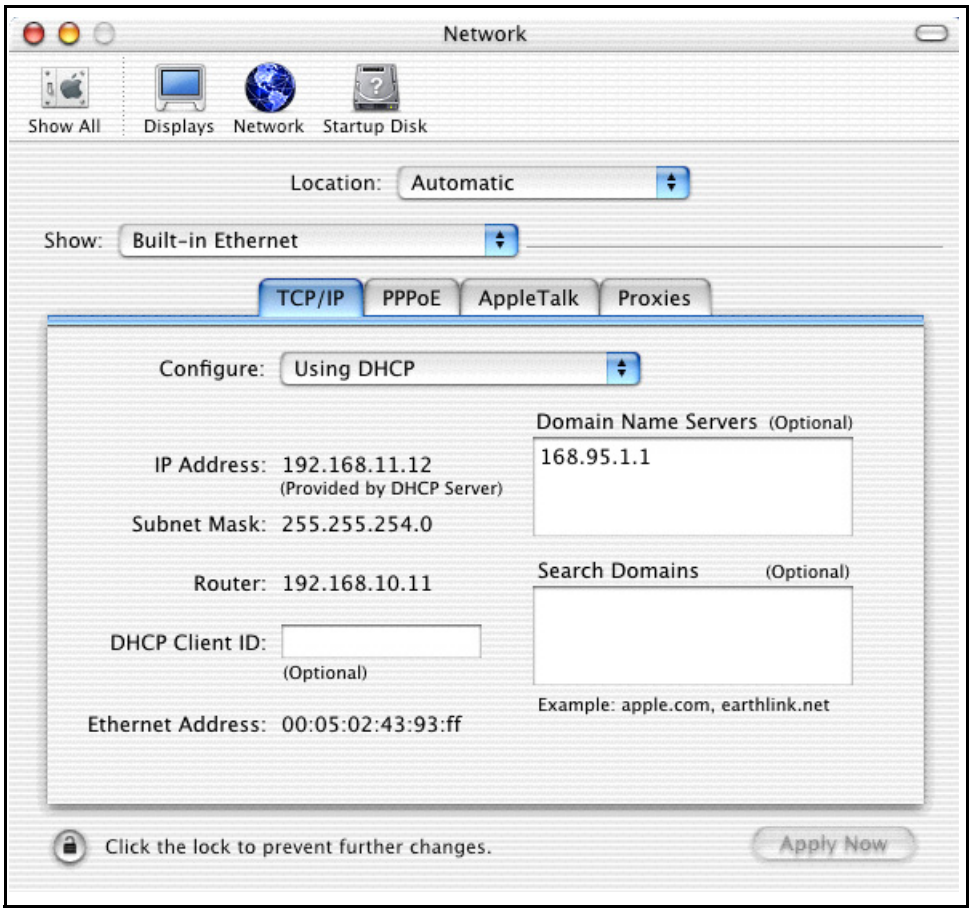
1 Нажмите кнопку меню **Apple** и затем **System Preferences (Настройки системы)**, чтобы открыть окно **System Preferences (Настройки системы)**.

Рис. 118 Macintosh OS X: Меню Apple



2 Нажмите **Network (Сеть)** на панели значков.
   - Выберите **Automatic (Автоматически)** в списке **Location (Местонахождение)**.
   - Выберите **Built-in Ethernet (Встроенный сетевой контроллер)** из списка **Show (Показать)**.
   - Выберите закладку **TCP/IP**.
3 Для настройки динамических параметров выберите **Using DHCP (Использовать DHCP)** в списке **Configure (Настроить)**.

Рис. 119 Macintosh OS X: Сеть



4 Для настройки статических параметров выполните следующие действия:
   - В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
   - Введите IP-адрес в окне **IP Address (IP-адрес)**.
   - Введите маску подсети в окне **Subnet mask (Маска подсети)**.
   - Введите IP-адрес интернет-центра в поле **Router address (Адрес маршрутизатора)**.
5 Нажмите **Apply Now (Применить)** и закройте окно.
6 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка настроек

Проверьте свойства TCP/IP в окне **Network (Сеть)**.

Linux

В этом разделе описана настройка TCP/IP Вашего компьютера в Red Hat Linux 9.0. Порядок настройки, диалоговые окна и размещение файлов могут различаться в зависимости от версии Linux.

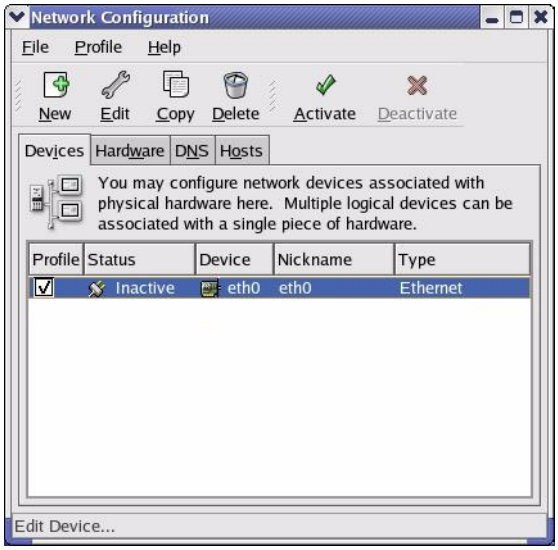
Вы должны быть зарегистрированы в системе в качестве корневого администратора.

Использование графического интерфейса KDE

Для настройки IP-адреса Вашего компьютера с помощью KDE проделайте следующее.

1 Нажмите кнопку **Red Hat** (в нижнем левом углу экрана), выберите **System Setting (Настройка системы)** и **Network (Сеть)**.

Рис. 120 Red Hat 9.0: KDE: Конфигурация сети: Устройства



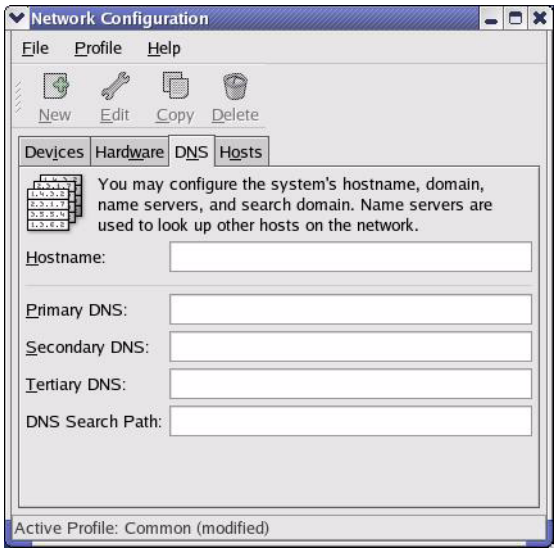
2 Дважды щелкните по профилю сетевой карты, которую Вы хотите настроить. При этом откроется окно **Ethernet Device – General (Устройство Ethernet – Общие)**.

Рис. 121 Red Hat 9.0: KDE: Устройство Ethernet: Общие

- Если у Вас динамический IP-адрес, нажмите **Automatically obtain IP address settings with (Автоматическое получение IP-адреса через...)** и из предложенного списка выберите **DHCP**.
- Если у Вас статический IP-адрес, нажмите **Statically set IP Addresses (Статическое присвоение IP-адреса)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Шлюз по умолчанию)**.

3. Нажмите **OK** для сохранения изменений и закройте окно **Ethernet Device – General**.
4. Если Вы знаете IP-адрес(а) сервера(ов) DNS, выберите вкладку **DNS** в окне **Network Configuration (Конфигурация сети)**. Введите данные серверов DNS в имеющиеся поля.

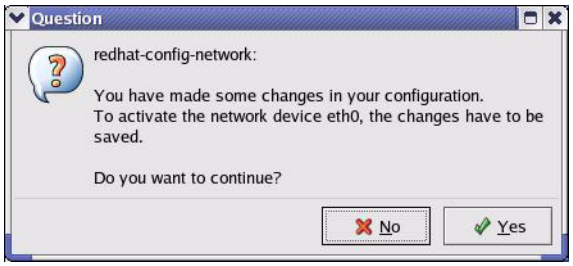
Рис. 122 Red Hat 9.0: KDE: Конфигурация сети: DNS



5 Выберите закладку **Devices (Устройства)**.

6 Нажмите кнопку **Activate (Активировать)** для вступления изменений в силу. Появится следующее окно. Нажмите **Да (Yes)**, чтобы сохранить изменения во всех окнах**.**

Рис. 123 Red Hat 9.0: KDE: Конфигурация сети: Включить



7 По завершении перезагрузки сетевой карты убедитесь, что **Status (Статус)** = **Active (Активен)** в окне **Network Configuration (Конфигурация сети)**.

Использование файлов конфигурации

Для редактирования файлов сетевой конфигурации и настройки IP-адреса Вашего компьютера выполните следующие действия:

1 Предположим, что Ваш компьютер оборудован только одной сетевой картой. Найдите файл конфигурации `ifconfig-eth0` (где `eth0` – имя карты Ethernet). Откройте его с помощью любого текстового редактора.

- Если у Вас динамический IP-адрес, то введите **`dhcp`** в поле **`BOOTPROTO=`**. Пример показан на следующем рисунке.

Рис. 124 Red Hat 9.0: Настройка динамического IP-адреса в файле «ifconfig-eth0»

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- Если у Вас статический IP-адрес, то введите **`static`** в поле **`BOOTPROTO=`**. Введите `IPADDR=`, затем IP-адрес (в десятичном виде с разделительными точками), `NETMASK=` и затем маску подсети. В приведенном ниже примере показан статический IP-адрес = 192.168.1.10 и маска подсети = 255.255.255.0.

Рис. 125 Red Hat 9.0: Настройка статического IP-адреса в файле «ifconfig-eth0»

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 Если Вы знаете IP-адрес(а) Вашего сервера DNS, то введите информацию о сервере DNS в файл `resolv.conf` в каталоге `/etc`. В следующем примере показан ввод двух IP-адресов сервера DNS.

Рис. 126 Red Hat 9.0: Установка параметров DNS в файле «resolv.conf»

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 После того как Вы отредактируете и сохраните файлы конфигурации, необходимо перезагрузить сетевую карту. Введите «`./network restart`» в каталоге `/etc/rc.d/init.d`. Пример показан на следующем рисунке.

Рис. 127 Red Hat 9.0: Перезапуск карты Ethernet

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

19.6.1 Проверка настроек

Чтобы проверить настройки TCP/IP, введите «`ifconfig`» в окне терминала.

Рис. 128 Red Hat 9.0: Проверка свойств протокола TCP/IP

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

E

Беспроводные локальные сети

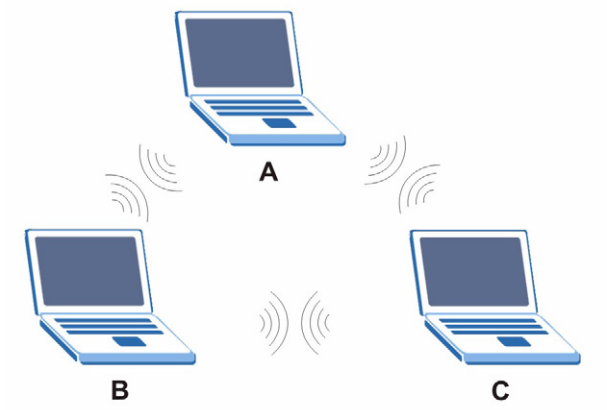
Топологии беспроводных локальных сетей

В этом разделе описаны временные (Ad-hoc) и фиксированные топологические схемы беспроводных локальных сетей.

Конфигурация временной (Ad-hoc) беспроводной локальной сети

Простейшей конфигурацией беспроводной локальной вычислительной сети (WLAN) является независимая (временная) WLAN, объединяющая группу компьютеров с беспроводными устройствами (A, B, C). Когда два или более беспроводных адаптеров попадают в зону действия друг друга, они могут образовать независимую сеть, обычно называемую «временной сетью» (Ad-hoc network) или «независимым базовым набором служб» (Independent Basic Service Set, IBSS). На приведенной диаграмме показан пример, где несколько ноутбуков используют беспроводные адаптеры для образования временной (Ad-hoc) беспроводной локальной сети.

Рис. 129 Одноранговая связь во временной (Ad-hoc) беспроводной сети

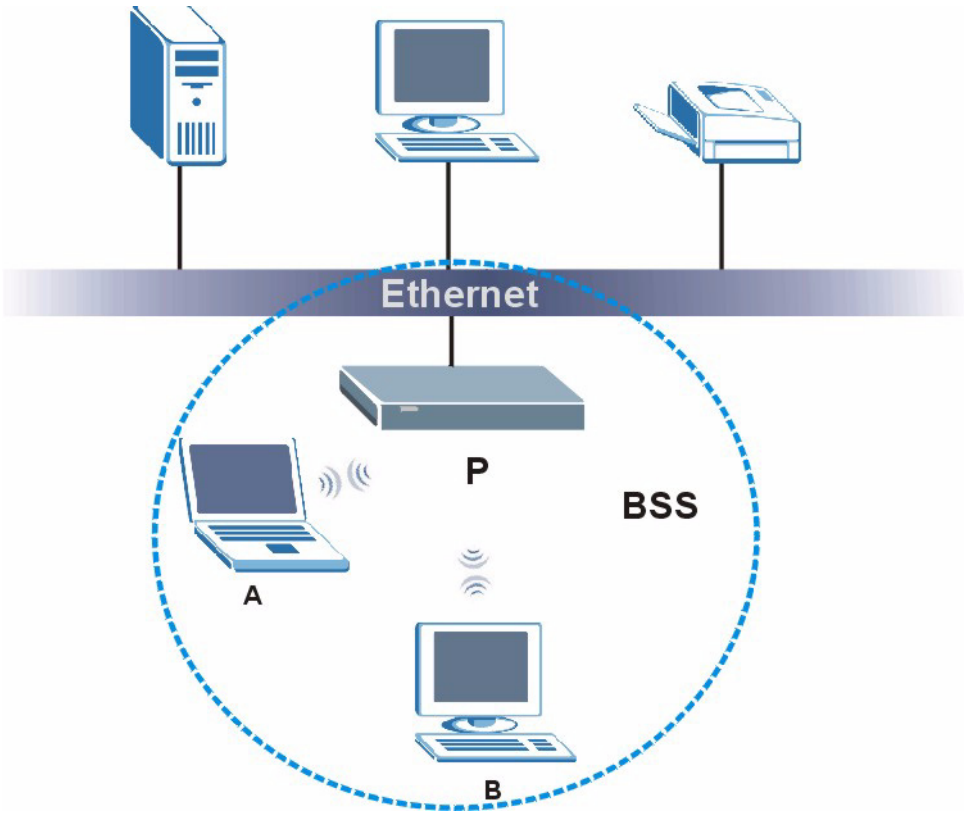


BSS (Базовый набор служб)

Базовый набор служб (BSS) существует тогда, когда весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети идет через одну точку доступа (AP).

Intra-BSS трафик – это трафик между беспроводными устройствами в пределах одного базового набора служб. При активации Intra-BSS трафика беспроводные устройства A и B могут получить доступ к проводной сети и обмениваться информацией между собой. При отключении Intra-BSS трафика беспроводные устройства A и B все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией между собой.

Рис. 130 Базовый набор служб



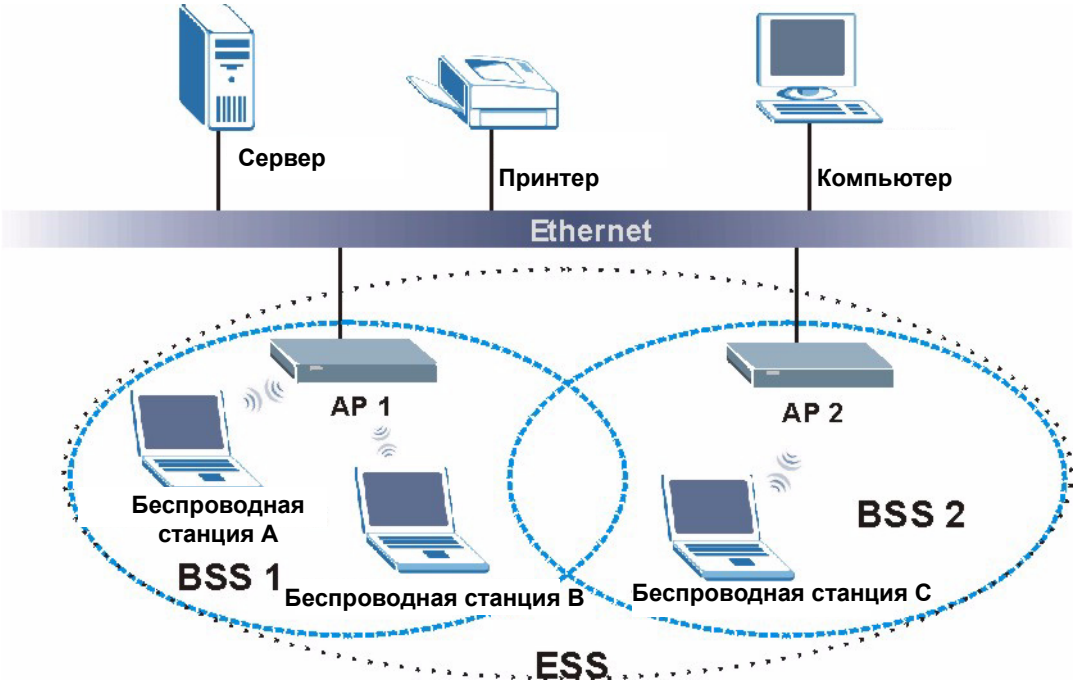
ESS

Расширенный набор служб (ESS) состоит из нескольких перекрывающихся базовых наборов служб (BSS), каждый из которых имеет точку доступа, а точки доступа связаны проводной сетью. Это проводное соединение точек доступа называется системой распределения (Distribution System, DS).

Этот тип беспроводной топологической организации локальной сети называется фиксированной беспроводной локальной сетью (Infrastructure WLAN). Точки доступа не только обеспечивают связь с проводной сетью, но и служат связующим звеном для трафика беспроводной локальной сети в непосредственном окружении.

Каждый ESS идентифицируется уникальным идентификатором (ESSID). Все точки доступа и связанные с ними беспроводные устройства в одном ESS должны иметь одинаковый идентификатор ESS.

Рис. 131 Фиксированная беспроводная сеть



Канал

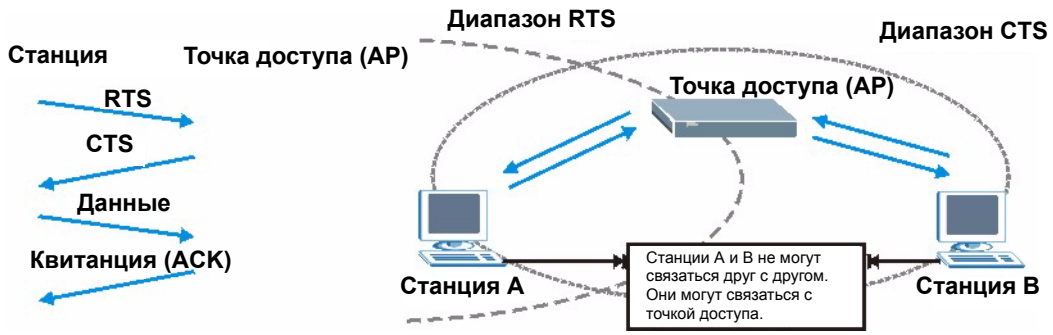
Канал представляет собой радиочастоту(ы), используемую(ые) беспроводными устройствами IEEE 802.11b/g. Доступность каналов зависит от географического положения. В некоторых регионах каналов может быть несколько, поэтому для снижения уровня помех следует использовать канал, отличающийся от канала ближайшей точки доступа. Помехи появляются при перекрывании радиосигналов от разных точек доступа, при этом ухудшается качество сигнала.

Однако смежные каналы частично перекрываются. Во избежание помех из-за перекрывания, канал точки доступа (AP) должен отстоять по крайней мере на пять каналов от частот, которые используют смежные точки доступа. Например, если в регионе действуют 11 каналов и смежная точка доступа использует канал 1, то Вам необходимо выбрать канал 6 или 11.

RTS/CTS (Запрос на передачу/Подтверждение готовности к приему)

«Скрытый» узел – это ситуация, когда два устройства находятся в рабочей зоне одной и той же точки доступа, но вне рабочих зон друг друга. Следующий рисунок иллюстрирует ситуацию «скрытого» узла. Оба устройства (STA) находятся в рабочей зоне точки доступа (AP) или беспроводного шлюза, но вне рабочих зон друг друга, поэтому они не могут «слышать» друг друга, т. е. они не знают, используется ли в данный момент канал. Поэтому они считаются скрытыми друг от друга.

Рис. 132 RTS/CTS



Когда устройство A посылает данные в точку доступа, оно может не знать, что устройство B уже использует канал. Если эти два устройства послали данные одновременно, может произойти конфликт, при котором обе партии данных достигают AP одновременно, результатом чего является потеря сообщений от обоих устройств.

RTS/CTS предназначен для предотвращения конфликтов из-за невидимых узлов. **RTS/CTS** определяет максимальный размер кадра данных, который можно отправить до квитирования (отправки запроса на передачу (RTS) и последующего получения подтверждения готовности к приему (CTS)).

Если кадр данных превышает значение **RTS/CTS**, установленное в диапазоне от 0 до 2432 байт, устройство, которое хочет передать этот кадр, должно вначале послать сообщение RTS (Request To Send – Запрос на передачу) точке доступа (AP) для получения разрешения на пересылку. Затем AP отвечает сообщением CTS (Clear to Send – Готовность к приему) всем другим устройствам в рабочей зоне, извещая их о необходимости задержки передачи данных. Для устройства, отправлявшего запрос, это сообщение одновременно подтверждает временные рамки, отведенные на передачу данных.

Кадры, меньше указанных в **RTS/CTS**, устройства могут посылать непосредственно в AP без квитирования (отправки запроса на передачу (RTS) и последующего получения подтверждения готовности к приему (CTS)).

Настройка **RTS/CTS** необходима только в случае, если существует вероятность наличия «скрытых» узлов в сети, а расходы на повторную отправку больших фрагментов оказываются больше, чем дополнительные сетевые издержки в связи с запросом разрешения на сеанс связи RTS (Request To Send – Запрос на передачу)/CTS (Clear to Send – Готовность к приему).

Если значение **RTS/CTS** превышает значение **порога фрагментации** (см. далее), квитирование RTS (Request To Send – Запрос на передачу)/CTS (Clear to Send – Готовность к приему) не будет иметь места, так как кадры данных будут фрагментированы до того, как достигнут размера **RTS/CTS**.

Включение порога RTS влечет за собой лишние сетевые издержки, которые зачастую негативно сказываются на пропускной способности, а не меняют ситуацию к лучшему.

Порог фрагментации

Порог фрагментации – это максимальный размер фрагмента данных (в диапазоне от 256 до 2432 байт), который может быть послан в беспроводную сеть, и при превышении которого точка доступа разделит пакет на меньшие кадры данных.

Большой **порог фрагментации** рекомендован для сетей, не склонных к помехам, тогда как для загруженных или склонных к помехам сетей необходимо установить меньший порог.

Если значение **порога фрагментации** меньше установленного значения **RTS/CTS** (см. ранее), квитирование RTS/CTS не будет иметь места, так как кадры данных будут фрагментированы до того как достигнут размера **RTS/CTS**.

Тип заголовка (Preamble Type)

Заголовок (вводная часть) используется для синхронизации времени передачи в беспроводной сети. Существует 2 режима заголовка: **длинный** и **короткий**.

Короткий заголовок требует меньше времени на обработку и минимизирует издержки, поэтому его следует использовать в хорошей беспроводной сети, если он поддерживается всеми беспроводными устройствами.

Режим **Long (Длинный заголовок)** следует выбрать в случае, если в сети высок уровень «шума» либо нет уверенности относительно того, какой режим заголовков поддерживают используемые беспроводные устройства (все беспроводные адаптеры стандарта IEEE 802.11b должны поддерживать длинные заголовки). Однако не все беспроводные адаптеры поддерживают короткие заголовки. Используйте длинный заголовок, если Вы не уверены, какой режим заголовков поддерживают беспроводные адаптеры. В этом случае будет гарантировано взаимопонимание между точкой доступа и беспроводными устройствами, и связь в сетях с высоким уровнем «шума» станет более надежной.

Выберите **Dynamic (Динамический)**, чтобы точка доступа автоматически использовала короткий заголовок, если он поддерживается всеми беспроводными устройствами, и длинный заголовок в остальных случаях.

Точка доступа и беспроводные устройства ДОЛЖНЫ использовать один и тот же режим заголовков.

Беспроводные локальные сети стандарта IEEE 802.11g

Стандарт IEEE 802.11g полностью совместим со стандартом IEEE 802.11b. Это означает, что адаптер IEEE 802.11b может непосредственно связываться с точкой доступа IEEE 802.11g (и наоборот) на скорости 11 Мбит/с или ниже, в зависимости от режима. IEEE 802.11g имеет несколько промежуточных вариантов скорости передачи между максимальной и минимальной скоростью передачи данных. Скорость передачи данных IEEE 802.11g и режим модуляции выглядят следующим образом:

Табл. 89 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	МОДУЛЯЦИЯ
1	DBPSK (Differential Binary Phase Shift Keyed – Кодирование дифференциальным двоичным сдвигом фазы)
2	DQPSK (Differential Quadrature Phase Shift Keying – Кодирование дифференциальным квадратурным сдвигом фазы)
5.5/ 11	CCK (Complementary Code Keying – Кодирование дополнительным кодом)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing – Ортогональное мультиплексирование с разделением частот)

IEEE 802.1x

В июне 2001 года был создан стандарт IEEE 802.1x, расширивший возможности стандарта IEEE 802.11, а именно поддерживающий расширенную аутентификацию и имеющий дополнительные функции учета и контроля. Он поддерживается Windows XP и рядом сетевых устройств. Вот некоторые из преимуществ IEEE 802.1x:

- Идентификация на уровне пользователей, обеспечивающая возможность роуминга.
- Поддержка системы RADIUS (Аутентификация удаленных пользователей по коммутируемым каналам связи, RFC 2138, 2139) для централизованного управления пользовательскими профилями и учетом на сетевом сервере RADIUS.
- Поддержка EAP (Расширяемого протокола аутентификации, RFC 2486), позволяющая использовать дополнительные методы аутентификации, не меняя настроек точки доступа и беспроводных устройств.

RADIUS

Система RADIUS основывается на модели «клиент-сервер», поддерживающей аутентификацию, авторизацию и учет. Клиент – это точка доступа, а сервер – это сервер RADIUS. Сервер RADIUS выполняет следующие задачи:

- Аутентификация
  Устанавливает подлинность пользователей.

- Авторизация

  Определяет сетевые службы, доступные для аутентифицированных пользователей после подключения к сети.
- Учет

  Отслеживает активность сети клиента.

RADIUS использует простой обмен пакетами, в котором точка доступа выступает в качестве ретранслятора сообщений между беспроводным устройством и сетевым сервером RADIUS.

Типы сообщений RADIUS

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях аутентификации пользователей:

- Access-Request (Доступ-Запрос)

  Посылается точкой доступа при запросе аутентификации.
- Access-Reject (Доступ-Отказ)

  Посылается сервером RADIUS при отказе в доступе.
- Access-Accept (Доступ-Разрешение)

  Посылается сервером RADIUS при разрешении доступа.
- Access-Challenge (Доступ-Приглашение)

  Посылается сервером RADIUS при запросе дополнительной информации для получения доступа. Точка доступа получает от пользователя надлежащий ответ, а затем посылает еще одно сообщение «Access-Request».

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS в целях учета пользователей:

- Accounting-Request (Учет-Запрос)

  Посылается точкой доступа при запросе учета.
- Accounting-Response (Учет-Ответ)

  Посылается сервером RADIUS и указывает, что учет начался или закончился.

Для обеспечения сетевой безопасности точка доступа и сервер RADIUS используют общий секретный ключ, который является паролем, известным им обоим. Этот ключ не передается по сети. Помимо общего секретного ключа, обмен информацией о пароле также кодируется для защиты сети от несанкционированного доступа.

Методы аутентификации

В этом приложении рассматриваются несколько распространенных типов аутентификации: **EAP-MD5, EAP-TLS, EAP-TTLS, PEAP** и **LEAP**.

Непосредственно используемый тип аутентификации зависит от сервера RADIUS и точки доступа. Подробную информацию можно получить у сетевого администратора.

EAP-MD5 (Алгоритм представления сообщения в краткой форме 5)

Аутентификация по методу MD5 – это простейший способ односторонней аутентификации. Сервер аутентификации отправляет беспроводному устройству запрос. Беспроводное устройство подтверждает знание пароля, для чего оно шифрует его и отправляет серверу в качестве ответа на запрос. Пароль не отправляется в виде обычного текста.

Однако метод MD5 имеет слабые стороны. Дело в том, что поскольку серверу аутентификации пароль нужен в виде обычного текста, его необходимо где-то сохранять. Следовательно, доступ к файлу с паролями может получить не только сервер аутентификации. Кроме того, сервер аутентификации можно сымитировать, т. е. выдать себя за него (поскольку метод MD5 не выполняет двусторонней аутентификации). И, наконец, метод MD5 не поддерживает шифрование данных с помощью динамического сеансового ключа. Чтобы зашифровать данные, необходимо настроить ключи шифрования WEP.

EAP-TLS (Безопасность на транспортном уровне)

При использовании метода EAP-TLS серверу и беспроводным устройствам для двусторонней аутентификации необходимы цифровые удостоверения. Сервер предоставляет клиентскому устройству свое удостоверение. После идентификации сервера клиентское устройство отправляет серверу свое удостоверение. До создания защищенного туннеля обмен удостоверениями производится в открытую. Это делает пользователя уязвимым для пассивных атак. Цифровое удостоверение – это электронная ID-карта, идентифицирующая отправителя. Однако для использования метода EAP-TLS необходимо иметь дело с центром сертификации (CA), которое занимается обработкой удостоверений, что влечет за собой административные издержки.

EAP-TTLS (Защита туннелированного транспортного уровня)

Метод EAP-TTLS представляет собой расширенную версию метода EAP-TLS. Для установления безопасного соединения удостоверения используются для аутентификации только со стороны сервера. Аутентификация клиента производится путем отправки имени пользователя и пароля через безопасное соединение (таким образом обеспечивается защита клиента). Метод EAP-TTLS поддерживает методы аутентификации клиента EAP и традиционные методы аутентификации, такие как PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (Защищенный EAP)

Как и в методе EAP-TTLS, для создания безопасного соединения здесь используется аутентификация удостоверений на стороне сервера, затем для аутентификации клиентов используются обычные методы проверки имени пользователя и пароля через созданное безопасное соединение. Таким образом защищаются персональные данные клиентов. Однако метод PEAP поддерживает лишь методы аутенификации клиента EAP, такие как EAP-MD5, EAP-MSCHAPv2 и EAP-GTC. Метод EAP-GTC реализует только корпорация Cisco.

LEAP (Упрощенный расширяемый протокол аутентификации)

LEAP (Упрощенный расширяемый протокол аутентификации) представляет собой протокол стандарта IEEE 802.1x, реализованный корпорацией Cisco.

Dynamic WEP Key Exchange (Динамический обмен ключами WEP)

Точка доступа копирует уникальный ключ, генерируемый сервером RADIUS. Этот ключ действителен до тех пор, пока беспроводное соединение не будет разорвано, не будет превышен лимит времени простоя, либо пока не истечет время простоя при повторной аутентификации. При каждой повторной аутентификации генерируется новый ключ WEP.

Если включить эту функцию, то настраивать ключ шифрования по умолчанию в окне **Wireless (Беспроводная сеть)** не обязательно. Вы можете создавать и сохранять ключи в этом окне, но они не будут использоваться при включенном режиме динамического шифрования WEP.

EAP-MD5 нельзя использовать для динамического обмена ключами WEP.

Для дополнительной безопасности методы аутентификации на основе цифровых удостоверений (EAP-TLS, EAP-TTLS и PEAP) используют динамические ключи для шифрования данных. Они часто используются в корпоративной среде, однако для применения в обычной среде более практичным оказывается традиционная пара «имя пользователя+пароль». В приведенной ниже таблице сравниваются функции различных методов аутентификации.

Табл. 90 Сравнительный анализ методов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Двусторонняя аутентификация	Нет	Да	Да	Да	Да
Удостоверение – Клиент	Нет	Да	По выбору	По выбору	Нет
Удостоверение – Сервер	Нет	Да	Да	Да	Нет
Динамический обмен ключами	Нет	Да	Да	Да	Да
Целостность мандата	Нет	Сильная	Сильная	Сильная	Средняя
Сложность применения	Низкая	Высокая	Средняя	Средняя	Средняя
Защита персональных данных клиентского устройства	Нет	Нет	Да	Да	Нет

WPA(2)

Wi-Fi Protected Access (WPA – Защищенный доступ Wi-Fi) представляет собой элемент из набора средств безопасности стандарта IEEE 802.11i. WPA2 (IEEE 802.11i) представляет собой безопасный стандарт беспроводной связи, обеспечивающий более защищенные по сравнению с WPA методы шифрования, аутентификации и управления ключами.

Основные отличия WPA(2) от WEP заключаются в более совершенных методах шифрования данных и аутентификации пользователя.

Шифрование

В WPA и WPA2 шифрование данных улучшено за счет использования протокола целостности временного ключа (TKIP), проверки целостности сообщения (MIC) и стандарта IEEE 802.1x. В дополнение к TKIP, в WPA2 используется расширенный стандарт шифрования (Advanced Encryption Standard – AES) в режиме счетчика и протокол кода аутентификации сообщения из цепочки цифровых блоков (Cipher block chaining Message authentication code Protocol – CCMP), что обеспечивает более криптостойкое шифрование.

Протокол шифрования с использованием временных ключей (Temporal Key Integrity Protocol – TKIP) использует 128-битные ключи, динамически создаваемые и распространяемые сервером аутентификации. Протокол поддерживает по-пакетное смешение ключей, проверку целостности пакетов (MIC), расширенный вектор инициализации (IV) с правилами упорядочения, а также механизм повторного генерирования ключей.

Протокол TKIP регулярно меняет и чередует ключи шифрования, так чтобы один и тот же ключ шифрования никогда не использовался дважды. Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает иерархию и систему управления ключами с использованием парного ключа для дальнейшего динамического генерирования уникальных ключей шифрования данных. Эти уникальные ключи используются для шифрования всех пакетов данных, передаваемых беспроводным методом между точкой доступа и беспроводными клиентами. Все это происходит автоматически в фоновом режиме.

WPA2 AES (Расширенный стандарт шифрования) представляет собой блочный шифр, использующий 256-битный математический алгоритм Rijndael.

Проверка целостности пакетов (MIC) предназначена для предотвращения перехвата, изменения и повторной отправки пакетов данных злоумышленниками. MIC имеет строгую математическую функцию, где принимающая и отправляющая стороны вычисляют каждая свой MIC, которые затем сравниваются. Если они не совпадают, то предполагается, что данные испорчены, и пакет удаляется.

При помощи генерирования уникальных ключей шифрования данных для каждого пакета данных и создания алгоритма проверки на целостность (MIC) протокол TKIP гораздо больше осложняет дешифрование данных в сети Wi-Fi по сравнению с WEP, затрудняя злоумышленнику проникновение в сеть.

Механизмы шифрования, используемые для WPA и WPA-PSK, одинаковы. Разница между WPA и WPA-PSK состоит в том, что WPA-PSK использует единственный предварительно согласованный ключ (пароль) для аутентификации всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Использование обычного пароля делает механизм WPA-PSK восприимчивым к атакам «грубой силы» с подбором пароля, но по сравнению с WEP он является более прогрессивным, поскольку здесь применяется более простой в использовании, постоянный буквенно-цифровой пароль.

Аутентификация пользователя

В WPA или WPA2 применяется стандарт IEEE 802.1x и протокол EAP (Extensible Authentication Protocol – Расширенный протокол аутентификации) для аутентификации беспроводных клиентов с использованием внешней базы данных RADIUS.

Если точка доступа и компьютеры беспроводных клиентов поддерживают WPA2 и имеется внешний сервер RADIUS, то следует использовать WPA2 для более совершенного шифрования данных. Если внешний сервер RADIUS отсутствует, следует использовать WPA2-PSK (ключ сети WPA2), который требует ввода только одного (одинакового) пароля для каждой точки доступа, беспроводного шлюза и компьютера беспроводного клиента. Если пароли совпадают, клиенту будет предоставлен доступ в беспроводную локальную сеть.

Если точка доступа или компьютеры беспроводных клиентов не поддерживают WPA2, следует использовать WPA или WPA-PSK, в зависимости от наличия внешнего сервера RADIUS.

Используйте WEP только в том случае, если точка доступа и/или беспроводные клиенты не поддерживают WPA или WPA2. WEP является менее надежным по сравнению с WPA или WPA2.

19.6.2 Пример применения WPA(2)-PSK

WPA(2)-PSK применяется следующим образом.

1. Сначала вводятся идентичные пароли для точки доступа и всех беспроводных устройств. Ключ сети (PSK) может содержать от 8 до 63 символов ASCII (включая пробелы и служебные символы).
2. Точка доступа проверяет пароль каждого беспроводного клиента и, если пароль совпадает, разрешает подключает к сети.
3. Точка доступа устанавливает и распределяет ключи для беспроводных клиентов.
4. Точка доступа и беспроводные клиенты используют протокол TKIP или стандарт AES для шифрования данных, передаваемых друг другу.

Рис. 133 Аутентификация WPA(2)-PSK

19.6.3 Пример применения WPA(2)-PSK с сервером RADIUS

Потребуются IP-адрес, номер порта (по умолчанию 1812) и общий секретный ключ сервера RADIUS. Далее приводится пример подключения по WPA(2) с использованием внешнего сервера RADIUS. «A» – это сервер RADIUS. «DS» – это система распределения.

1. Точка доступа посылает запрос серверу RADIUS на аутентификацию беспроводного клиента.
2. Сервер RADIUS проводит идентификацию пользователя по своей базе данных и либо предоставляет, либо запрещает доступ в сеть (в соответствии с результатом аутентификации).
3. Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает иерархию и систему управления ключами с использованием парного ключа для дальнейшего динамического генерирования уникальных ключей шифрования данных. Эти уникальные ключи используются для шифрования всех пакетов данных, передаваемых беспроводным методом между точкой доступа и беспроводными клиентами.

Обзор параметров безопасности

В этой таблице приведены прочие параметры безопасности, которые нужно настроить для каждого метода аутентификации/протокола управления ключами. Фильтры MAC-адресов не зависят от настройки этих характеристик безопасности.

Табл. 91 Сравнительная таблица беспроводной безопасности

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	РУЧНОЙ ВВОД КЛЮЧА	IEEE 802.1X
Открытый	Нет	Нет	Отключен
			Включен с динамическим ключом WEP
Открытый	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
Коллективный	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
WPA	TKIP	Нет	Включен
WPA-PSK	TKIP	Да	Включен
WPA2	AES	Нет	Включен
WPA2-PSK	AES	Да	Включен

F

Службы

В следующей таблице содержатся распространенные службы и связанные с ними протоколы и номера портов.

- **Имя**: короткое описательное имя службы. Можно использовать это имя или создать другое.
- **Протокол**: тип протокола протокол IP, используемый для данной службы. Если используется **TCP/UDP**, то служба использует одинаковый с TCP и UDP номер порта. Если используется **USER-DEFINED (Определяется пользователем)**, параметр **Port(s) (Порт(ы))** является номером протокола IP, не номером порта.
- **Порт(ы)**: значение зависит от параметра **Протокол**.
  - Если значение **Протокола** – **TCP**, **UDP**, или **TCP/UDP**, то это номер порта IP.
  - Если значение **Протокола** – **USER**, то это номер протокола IP.
- **Описание**: краткое описание приложений, которые используют данную службу, или ситуацией, в которых используется данная служба.

Табл. 92 Примеры служб

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Определяется пользователем	51	Эту службу использует протокол туннелирования IPSEC AH (Заголовок аутентификации).
AIM	TCP	5190	Служба Internet Messenger AOL.
AUTH	TCP	113	Протокол аутентификации, используется некоторыми серверами.
BGP	TCP	179	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT	UDP	68	Клиент DHCP.
BOOTP_SERVER	UDP	67	Сервер DHCP.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	Популярное решение для проведения видеоконференций от White Pines Software.
DNS	TCP/UDP	53	Сервер имен доменов – служба, определяющая соответствие web-имен (например, www.zyxel.com) и номеров IP.
ESP (IPSEC_TUNNEL)	Определяется пользователем	50	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).

Табл. 92 Примеры служб (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
FINGER	TCP	79	Finger – команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.
FTP	TCP TCP	20 21	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.
H.323	TCP	1720	Протокол для Net Meeting.
HTTP	TCP	80	Протокол передачи гипертекста – протокол уровня клиент/сервер для WWW.
HTTPS	TCP	443	HTTPS – это надежный сеанс связи http, часто используемый в электронной коммерции.
ICMP	Определяется пользователем	1	Internet Control Message Protocol (Протокол межсетевых управляющих сообщений) часто используется в целях диагностики.
ICQ	UDP	4000	Популярная система интерактивного общения в Интернет.
IGMP (многоадресная рассылка)	Определяется пользователем	2	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отправки пакетов определенным группам узлов.
IKE	UDP	500	Алгоритм обмена ключами в Интернет, используется для распределения и управления ключами.
IMAP4	TCP	143	Internet Message Access Protocol 4 (Протокол интерактивного доступа к электронной почте, версия 4).
IMAP4S	TCP	993	Более защищенная версия протокола IMAP4, работающая через SSL-соединение.
IRC	TCP/UDP	6667	Еще одна программа интерактивного общения в Интернет.
MSN Messenger	TCP	1863	Протокол для передачи сообщений в сетях Microsoft.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	Network Basic Input/Output System (Сетевая базовая система ввода-вывода), используется для взаимодействия компьютеров в локальной сети.
NEW-ICQ	TCP	5190	Программа для обмена текстовыми сообщениями между абонентами сети Internet в реальном времени.
NEWS	TCP	144	Протокол для групп новостей.

Табл. 92 Примеры служб (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
NFS	UDP	2049	Сетевая файловая система – NFS, распределенная файловая служба клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сети.
NNTP	TCP	119	Network News Transport Protocol (Сетевой протокол передачи новостей) – система доставки для групп новостей USENET.
PING	Определяется пользователем	1	Packet INternet Groper (Пакетное эхо-тестирование в Интернет) – это протокол, который посылает эхо-запросы ICMP для проверки достижимости удаленного узла.
POP3	TCP	110	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
POP3S	TCP	995	Более защищенная версия протокола POP3, работающая через SSL-соединение.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал управления.
PPTP_TUNNEL (GRE)	Определяется пользователем	47	PPTP (Point-to-Point Tunneling Protocol – Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал передачи данных.
RCMD	TCP	512	Удаленное управление командной строкой.
REAL_AUDIO	TCP	7070	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в сети в реальном времени.
REXEC	TCP	514	Daemon-служба удаленного выполнения команд.
RLOGIN	TCP	513	Удаленная регистрация.
ROADRUNNER	TCP/UDP	1026	Поставщик Интернет-услуг, предоставляющий их, в основном, через кабельные модемы.
RTELNET	TCP	107	Удаленный доступ через Telnet.
RTSP	TCP/UDP	554	Протокол (Real Time Streaming – Протокол воспроизведения в реальном времени) – это удаленное управление для мультимедиа в Интернете.
SFTP	TCP	115	Simple File Transfer Protocol (Простой протокол передачи файлов) – устаревший способ обмена файлами между компьютерами.

Табл. 92 Примеры служб (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SMTP	TCP	25	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SMTPS	TCP	465	Более защищенная версия протокола SMTP, работающая через SSL-соединение.
SNMP	TCP/UDP	161	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS	TCP/UDP	162	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language (Язык структурированных запросов) представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, системы средней производительности, системы UNIX и сетевые серверы.
SSDP	UDP	1900	Simple Service Discovery Protocol supports Universal Plug-and-Play (Протокол обнаружения подключенных периферийных устройств на основе Plug & Play).
SSH	TCP/UDP	22	Программа безопасной удаленной регистрации.
STRM WORKS	UDP	1558	Протокол передачи потоков Stream Works.
SYSLOG	UDP	514	Системный журнал – позволяет отправлять журналы системы серверу UNIX.
TACACS	UDP	49	Login Host Protocol (Протокол регистрации узла), используется для TACACS (Terminal Access Controller Access Control System – Система управления доступом на основе контроллера доступа к терминалу).
Сетевой теледоступ (Telnet)	TCP	23	Telnet – протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах.

Табл. 92 Примеры служб (продолжение)

NAME (ИМЯ)	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
TFTP	UDP	69	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE	TCP UDP	7000 Определяется пользователем	Решение для проведения видеоконференций. Номер порта UDP задается в приложении.

G

Сервисная служба

При обращении в Сервисную службу будьте готовы предоставить следующую информацию:

Обязательные сведения

- Модель изделия и серийный номер.
- Гарантийные обязательства.
- Дата приобретения устройства.
- Краткое описание неисправности, а также действий, предпринятых по ее устранению.

Вместо “+” наберите код международной телефонной связи.

Головной офис корпорации (по всему миру)

- E-mail службы поддержки: support@zyxel.com.tw
- E-mail отдела продаж: sales@zyxel.com.tw
- Телефон: +886-3-578-3942
- Факс: +886-3-578-2439
- Web-сайт: www.zyxel.com, www.europe.zyxel.com
- FTP-сервер: ftp.zyxel.com, ftp.europe.zyxel.com
- Обычная почта: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Великобритания

- E-mail службы поддержки: support@zyxel.co.uk
- E-mail отдела продаж: sales@zyxel.co.uk
- Телефон: +44-1344-303044, 08707-555779 (только Великобритания)
- Факс: +44-1344-303034
- Web-сайт: www.zyxel.co.uk
- FTP-сервер: ftp.zyxel.co.uk
- Обычная почта: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

3.

Венгрия

- E-mail службы поддержки: support@zyxel.hu
- E-mail отдела продаж: info@zyxel.hu
- Телефон: +36-1-3361649
- Факс: +36-1-3259100
- Web-сайт: www.zyxel.hu
- Обычная почта: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Германия

- E-mail службы поддержки: support@zyxel.de
- E-mail отдела продаж: sales@zyxel.de
- Телефон: +49-2405-6909-69
- Факс: +49-2405-6909-99
- Web-сайт: www.zyxel.de
- Обычная почта: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Дания

- E-mail службы поддержки: support@zyxel.dk
- E-mail отдела продаж: sales@zyxel.dk
- Телефон: +45-39-55-07-00
- Факс: +45-39-55-07-07
- Web-сайт: www.zyxel.dk
- Обычная почта: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Индия

- E-mail службы поддержки: support@zyxel.in
- E-mail отдела продаж: sales@zyxel.in
- Телефон: с +91-11-30888144 по +91-11-30888153
- Факс: +91-11-30888149, +91-11-26810715
- Web-сайт: http://www.zyxel.in
- Обычная почта: Индия – ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Испания

- E-mail службы поддержки: support@zyxel.es
- E-mail отдела продаж: sales@zyxel.es
- Телефон: +34-902-195-420
- Факс: +34-913-005-345
- Web-сайт: www.zyxel.es
- Обычная почта: ZyXEL Communications, Arte, 21 5Є planta, 28033 Madrid, Spain

Казахстан

- Служба поддержки: http://zyxel.kz/support
- E-mail отдела продаж: sales@zyxel.kz
- Телефон: +7-3272-590-698
- Факс: +7-3272-590-689
- Web-сайт: www.zyxel.kz
- Обычная почта: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

Коста-Рика

- E-mail службы поддержки: soporte@zyxel.co.cr
- E-mail отдела продаж: sales@zyxel.co.cr
- Телефон: +506-2017878
- Факс: +506-2015098
- Web-сайт: www.zyxel.co.cr
- FTP-сервер: ftp.zyxel.co.cr
- Обычная почта: ZyXEL Costa Rica, Plaza Roble Escazъ, Etapa El Patio, Tercer Piso, San Josй, Costa Rica

Малайзия

- E-mail службы поддержки: support@zyxel.com.my
- E-mail отдела продаж: sales@zyxel.com.my
- Телефон: +603-8076-9933
- Факс: +603-8076-9833
- Web-сайт: http://www.zyxel.com.my
- Обычная почта: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

Норвегия

- E-mail службы поддержки: support@zyxel.no
- E-mail отдела продаж: sales@zyxel.no
- Телефон: +47-22-80-61-80
- Факс: +47-22-80-61-81
- Web-сайт: www.zyxel.no
- Обычная почта: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Польша

- E-Mail: info@pl.zyxel.com
- Телефон: +48-22-333 8250
- Факс: +48-22-333 8251
- Web -сайт: www.pl.zyxel.com
- Обычная почта: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Россия

- Служба поддержки: http://zyxel.ru/support
- E-mail отдела продаж: sales@zyxel.ru
- Телефон: +7-095-542-89-29
- Факс: +7-095-542-89-25
- Web-сайт: www.zyxel.ru
- Обычная почта: Россия, 117279, г. Москва, ул. Островитянова, 37а

Северная Америка

- E-mail службы поддержки: support@zyxel.com
- E-mail отдела продаж: sales@zyxel.com
- Телефон: +1-800-255-4101, +1-714-632-0882
- Факс: +1-714-632-0858
- Web-сайт: www.us.zyxel.com
- FTP-сервер: ftp.us.zyxel.com
- Обычная почта: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Сингапур

- E-mail службы поддержки: support@zyxel.com.sg
- E-mail отдела продаж: sales@zyxel.com.sg
- Телефон: +65-6899-6678
- Факс: +65-6899-8887
- Web-сайт: http://www.zyxel.com.sg
- Обычная почта: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Таиланд

- E-mail службы поддержки: support@zyxel.co.th
- E-mail отдела продаж: sales@zyxel.co.th
- Телефон: +662-831-5315
- Факс: +662-831-5395
- Web-сайт: http://www.zyxel.co.th
- Обычная почта: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Украина

- E-mail службы поддержки: support@ua.zyxel.com
- E-mail отдела продаж: sales@ua.zyxel.com
- Телефон: +380-44-247-69-78
- Факс: +380-44-494-49-32
- Web-сайт: www.ua.zyxel.com
- Обычная почта: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

Финляндия

- E-mail службы поддержки: support@zyxel.fi
- E-mail отдела продаж: sales@zyxel.fi
- Телефон: +358-9-4780-8411
- Факс: +358-9-4780-8448
- Web-сайт: www.zyxel.fi
- Обычная почта: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

Франция

- E-Mail: info@zyxel.fr
- Телефон: +33-4-72-52-97-97
- Факс: +33-4-72-52-19-20
- Web-сайт: www.zyxel.fr
- Обычная почта: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Чешская Республика

- E-Mail: info@cz.zyxel.com
- Телефон: +420-241-091-350
- Факс: +420-241-091-359
- Web-сайт: www.zyxel.cz
- Обычная почта: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 – Modrany, Ceská Republika

Швеция

- E-mail службы поддержки: support@zyxel.se
- E-mail отдела продаж: sales@zyxel.se
- Телефон: +46-31-744-7700
- Факс: +46-31-744-7701
- Web-сайт: www.zyxel.se
- Обычная почта: ZyXEL Communications A/S, Sjцporten 4, 41764 Gцteborg, Sweden

Япония

- E-mail службы поддержки: support@zyxel.co.jp
- E-mail отдела продаж: sales@zyxel.co.jp
- Телефон: +81-3-6847-3700
- Факс: +81-3-6847-3705
- Web-сайт: www.zyxel.co.jp
- Обычная почта: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Алфавитный указатель

0 – 9

802.11 Mode (Режим 802.11) 58

A

ActiveX 114
Alert (Предупреждение) 167

B

BitTorrent 128
BSS (Базовый набор служб) 238

C

CA (Центр сертификации) 244
Configuration (Настройка) 185
  Восстановление 186
  Восстановление заводских настроек 187
  Резервное копирование 185
Cookies 114
CTS (Готовность к приему) 240

D

Daylight Saving (Переход на летнее время) 162
DDNS 99
  см. также «Динамическая система доменных имен»
DHCP 26, 83
  Сервер DHCP
  см. также «Протокол динамической настройки узла»
DHCP Server (Сервер DHCP) 77
DNS 85
DNS (Domain Name System – Система доменных имен) 143
Dynamic WEP Key Exchange (Динамический обмен ключами WEP) 245

E

E-Mail 61
ESS 238
ESSID 194

F

FTP 14, 142
FTP. см. также «Программа передачи файлов» 127

H

HTTP 128

I

IANA (Агентство по назначению имен и уникальных параметров протоколов Интернет) 219
IBSS (Независимый базовый набор служб) 237
IEEE 802.11g 242
IGMP 63, 78
  версия 63
  см. также «Протокол многоадресной рассылки» 63
  см. также «широковещательный про
IP Address (IP-адрес) 80, 91
IP-адрес 91

J

Java 114

L

LAN 77
  Настройка диапазона IP-адресов 77
Log (Регистрационный журнал) 165

M

MAC (Управление доступом к среде) 55
MAC-адрес 42, 55, 63
  Копирование 63
MAC-адрес порта WAN 63
Metric (Метрика) 123
MSN Messenger 128
MSN Webcam 128

N

NAT 89, 91
  Наборы серверов 89
  Обзор 89
  Переадресация портов 89
  см. также «Трансляция сетевых адресов»
NAT (Трансляция сетевых адресов) 219
NAT Traversal 145
NetBIOS 75, 82
  см. также «сетевая базовая система ввода-вывода» 75
Network Basic Input / Output System (сетевая базовая система ввода-вывода) 82

P

P2P 128
Pool Size (Размер пула) 84
Port Speed (Скорость порта) 21
PPTP 70
Private (Частный адрес) 123

Q

QoS (Качество услуг) 46

R

RADIUS 242
  Общий секретный ключ 243
ROADRUNNER 65
RTS (Запрос на передачу) 240
RTS Threshold (Порог RTS) 240, 241
RTS/CTS Threshold (RTS/CTS Порог) 57

S

SIP 127
SMTP 169
SNMP 106
SSID 20, 40, 48
System Name (Системное имя) 159

T

Telnet 141

U

UPnP 145
  Вопросы безопасности 146
  Форум 146

V

VoIP 127
VPN 70

W

Web Proxy 114
Web-конфигуратор 14
  Доступ 17
  Обзор 17
  Работа с интерфейсом 19
WEP key (Ключ WEP) 49
WEP-шифрование 49, 50

WLAN (Беспроводная локальная сеть)
Параметры безопасности 249
Помехи 239
WMM 46
WPA Compatible (Совместимость с WPA) 44
WPA, WPA2 246
WWW 61, 128

X

Xbox Live 127

А

Агентство по назначению имен и уникальных параметр
Альтернативные варианты записи маски подсети 214
Асимметричные маршруты 107
и псевдоним IP 107
см. также «треугольные маршруты» 107
Аутентификация
EAP 243
Аутентификация пользователя 42, 247
Локальная база данных пользователей 43
Сервер RADIUS 43

Б

Безопасность беспроводной сети 194
Беспроводная локальная сеть 194
Беспроводная сеть
SSID 40
Безопасность 40
Канал 40
Обзор 39
Пример 39
Принципы 40
Фильтрация MAC-адресов 42
Шифрование 43
Беспроводной канал 194
Блокировка по ключевым словам в URL 115

В

Версия микропрограммы 20
Версия протокола IGMP 63, 78
Влажность 199
Восстановление конфигурации 186
«Всемирная паутина» 128
Выходная мощность 58

Г

Габариты 199

Д

Динамическая система доменных имен 99
Дополнительные настройки WAN 74
Дуплексный режим 21

З

Загрузка микропрограммы 183
Расширение файла
Через HTTP
Загрузка центрального процессора 21
Защита беспроводной связи 40
Обзор 42
Тип 42

И

Идентификатор набора служб 48
Идентификатор набора служб См. SSID
Имя пользователя 100
Инициация переадресации портов 94
Пример 95
Процесс 95
Интерфейс командной строки 14
Информация о клиентах DHCP 86
Использование памяти 21

К

Канал 20, 40, 239
  Помехи 239
Качество предоставления услуг в беспроводной среде передачи 46
Качество услуг (QoS) 58
Кнопка Reset (Сброс) 187
Кнопка Reset (Сброс) 18
Контактная информация 257

Л

Локальная база данных пользователей 43
  и шифрование 44
Локальная вычислительная сеть 77

М

Маска подсети 80, 212
Межсетевой экран 105
  Инспекция пакетов с учетом состояния 105
  Межсетевой экран – общая информация
  Межсетевой экран, встроенный в устройство ZyXEL 106
  Пакеты ICMP 109
  Руководства 106
  Сетевая безопасность 105
Многоадресная рассылка 63, 78
  IGMP 63, 78
Мониторинг управления пропускной способностью 26

Н

Набор служб 48
Настройка TCP/IP 83
Настройка TCP/IP локальной сети 77
Настройка локальной сети 63, 77
Независимый базовый набор служб 237

О

Общая информация о локальной сети 77
Общая настройка системы 159
Ограничение веб-функций 114
Окно общих настроек беспроводной сети 47
Организация подсетей 214
Организация сети в Windows 82

П

Панель навигации 23
Параметры безопасности 249
Пере
Переадресация портов 89, 91
  локальный сервер 91
  Пример 90
  Сервер по умолчанию 90
  Службы
Передача IP-пакетов 78
  Многоадресная
  Одноадресная
Перезапуск системы 187
Питание 199
Подсеть 211
Порог фрагментации 57, 241
Порт инициации 94
Приоритеты 46
Приоритеты QoS 46
Приоритеты WMM 46
Программа передачи файлов 127
Простой протокол передачи файлов. 169
Протокол динамической настройки узла 83
Протокол инициации сеанса 127
Протокол многоадресной рассылки 63, 78
Протокол передачи гипертекста 128
Протокол разрешения адресов (ARP) 79
Протокол туннелирования «точка-точка» 70
Псевдоним IP 80
Пул IP-адресов 84

Р

Рабочий канал 20
Радиочастота (RF) 200
Расширенный набор служб 238
Режим заголовка 241
Резервное сохранение конфигурации 185
Роуминг 44, 57
  Требования 45

С

Сброс настроек устройства 18
Сводка 26
  Мониторинг управления пропускной способностью 26
  Состояние беспроводных станций 29
  Статистика передачи пакетов 28
  Таблица DHCP 26
Сервер DHCP 83
Сервер DNS 85
Сервер RADIUS 43
Сервисная служба 257
Сетевая операционная система ZyXEL (ZyNOS) 20
Скрытый узел 240
Служба имен доменов 85
Службы
  и номера портов 251
  и протоколы 251
Службы и номера портов 128
Сообщения RADIUS 243
Сопроводительная документация 3
сопроводительная документация 3
Состояние 19
Список беспроводных подключений 29
Список клиентов DHCP 86
Статический маршрут 121
  и удаленный узел
  Обзор
Статическое DHCP 84

Т

Таблица DHCP 26, 86
  Информация о клиентах DHCP
  Состояние DHCP
Температура 199
Техника безопасности 7
Тип соединения 21
Типы сообщений RADIUS 243
Точка доступа (AP) 239
Точка-точка 128
Трансляция сетевых адресов 89, 91
Треугольные маршруты
  и псевдоним IP 107
  см. также «Асимметричные маршруты» 107

У

Удаленное управление 139
  FTP 142
  Время простоя системы 140
  и NAT 140
  и межсетевой экран 139
  Ограничения 140
  Сеанс удаленного управления 140
Универсальная функция Plug and Play 145
  Применение 145
Управление пропускной способностью
  Классы и приоритеты 130
  Монитор 137
  На основе подсетей 126
  На основе приложений 126
  Обзор 125
  Приоритет 127
  Службы 127
Управление устройством
  Использование интерфейса командной строки
    См. интерфейс командной строки.
  Полезные советы 14
  С использованием FTP. См. FTP
  С использованием Web-конфигуратора. см. Web-конфигуратор.
Условные обозначения 5
Установка UPnP 147
  Windows Me 147
  Windows XP 149
Установка времени 161
Учебное руководство по развертыванию беспроводной сети 31

Ф

Фильтр MAC-адресов 55
Фильтрация MAC-адресов 42, 55
Фильтрация на основе содержания
  График блокирования 113
  Ограничение веб-функций 113
Функция Any IP (Любой IP)
  Примечание 79

Ц

Центр сертификации 244

Ш

Шаблон 99
Шаблон DynDNS 99
Шифрование 43, 246
  WPA Compatible (Совместимость с WPA) 44
  и локальная база данных пользователей 44
  Ключ 44
Шлюз 122